ESTUDIO DE PERCEPCIÓN
Seguridad en Informática México 2007

Joint Future Systems ha llevado a cabo el Estudio de Percepción sobre Seguridad en Informática México 2007, con el propósito de generar estadísticas del entorno de nuestro país en la materia y de contar con parámetros comparativos que permitan vislumbrar las variaciones (avances o rezagos percibidos por los entrevistados), contra los estudios realizados en 2004 y 2005.

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

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

B) Estudio de opinión y análisis con 17 expertos en temas relacionados con seguridad en informática.

C) Artículos de interés, relacionados con seguridad en informática.

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

Levantamiento de información y opiniones de 1,081 ejecutivos de diferentes niveles, pertenecientes a empresas privadas de diversos sectores, empresas paraestatales, dependencias gubernamentales, instituciones educativas, cámaras y asociaciones.

B) Estudio de opinión y análisis con expertos en temas relacionados con seguridad en informática

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

Organizaciones patrocinadoras

- Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI)
- CA Software de México
- Cámara Mexicano-Alemana de Comercio e Industria (CAMEXA)
- Cámara Nacional de la Industria Electrónica de Telecomunicaciones e Informática (CANIETI)
- International Association of Financial Crimes Investigators (IAFCI) Capítulo México
- Intel México
- Joint Future Systems
- QoS Labs de México
- Sun Microsystems de México
- Técnica Comercial Vilsa
- Tralix

JFS

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

CONTENIDO

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
La metodología de levantamiento de encuestas se realizó en 2 etapas, una a través de correo electrónico y la otra por medio de llamadas telefónicas.

Encuestas vía correo electrónico
Las encuestas fueron realizadas en el periodo que abarca del 3 de Octubre al 15 de noviembre de 2006.

Encuestas telefónicas
Las encuestas fueron realizadas en el periodo que abarca del 15 de noviembre de 2006 al 8 de enero de 2007.

Instrumento de medición
Para ambas fuentes de levantamiento de información, se aplicó un cuestionario estructurado, exactamente con las mismas preguntas, adaptadas a cada medio.

Características de la muestra

• Perfil de los entrevistados

Característica principal	Directivos y niveles medios de diferentes áreas organizacionales, como son Direcciones Generales, Sistemas, Administración y Finanzas, según dimensiones y características de la Organización.
Edad:	Indistinta
Sexo:	Indistinto
Cobertura geográfica:	Múltiple, dentro de la República Mexicana
N.S.E.	Indistinto

• Campo de muestreo

Se utilizaron diversas bases de datos públicas y diversas listas de correo electrónico.

• Tamaño de la muestra

481 respuestas por correo electrónico (28 informáticos, 453 no-informáticos).

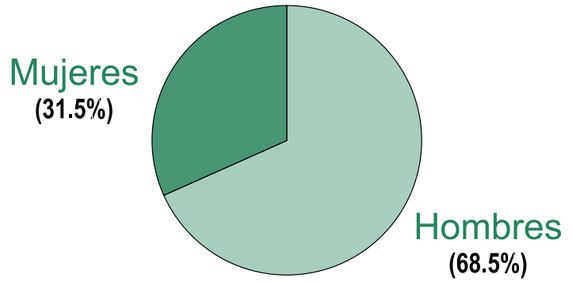
600 respondentes por teléfono. (250 informáticos, 350 no-informáticos).

Total informáticos	278
Total No Informáticos	803
Total entrevistados	1,081

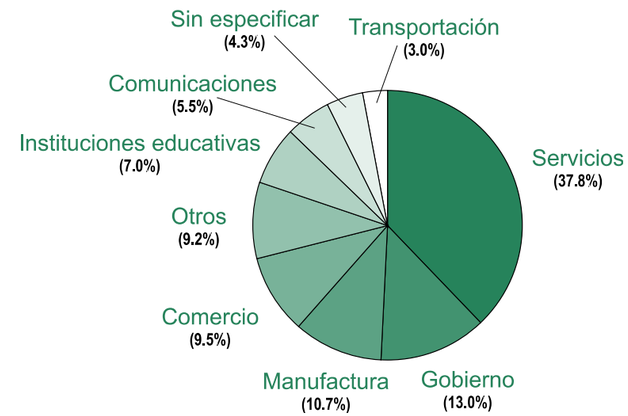
• Codificación de respuestas

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

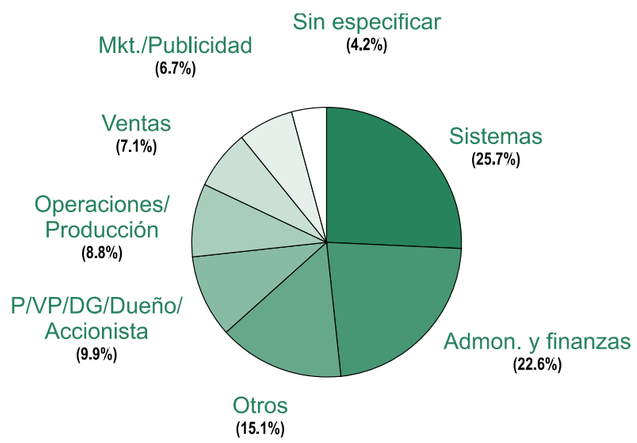
COMPOSICIÓN DE LA MUESTRA POR SEXO



COMPOSICIÓN DE LA MUESTRA POR SECTOR



COMPOSICIÓN DE LA MUESTRA POR PUESTO/ÁREA



* **P/VP/DG/Dueño/ Accionista.-** Este perfil contempla puestos como Presidente, Vicepresidente, Director General, Consejero, Dueño de la empresa, Accionista, etc.

• 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 (1.55 respuestas promedio por entrevistado). La frecuencia de las respuestas ya codi -ficadas, puede apreciarse en la Tabla 1 y la Gráfica 4.

JFS

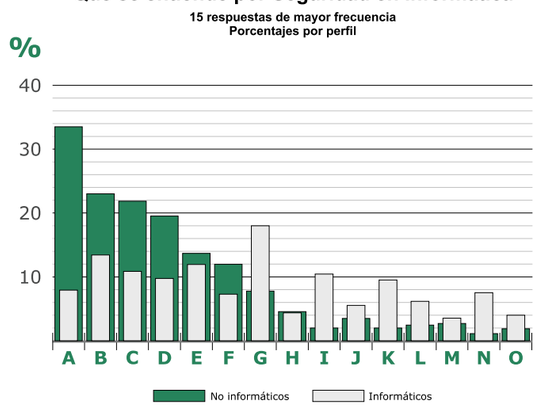
TABLA 1

Qué se entiende por seguridad en Informática

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Privacidad / Confidencialidad	268	22	290	33.4%	7.9%	24.8%	2.0%	26.8%
Transmisión segura de datos	183	37	220	22.8%	13.3%	16.9%	3.4%	20.4%
Medidas de seguridad en general (sin especificar)	176	30	206	21.9%	10.8%	16.3%	2.8%	19.1%
Protección contra virus	157	27	184	19.6%	9.7%	14.5%	2.5%	17.0%
Integridad / Confiabilidad de la información	110	33	143	13.7%	11.9%	10.2%	3.1%	13.2%
Protección contra hackers	96	20	116	12.0%	7.2%	8.9%	1.9%	10.7%
Acceso controlado	62	50	112	7.7%	18.0%	5.7%	4.6%	10.4%
Protección contra spyware	36	12	48	4.5%	4.3%	3.3%	1.1%	4.4%
Políticas adecuadas / procedimientos / uso responsable	16	29	45	2.0%	10.4%	1.5%	2.7%	4.2%
Manejo de Identidad	28	15	43	3.5%	5.4%	2.6%	1.4%	4.0%
Respaldo de información	15	26	41	1.9%	9.4%	1.4%	2.4%	3.8%
Protección contra spam	19	17	36	2.4%	6.1%	1.8%	1.6%	3.3%
Cuidado de los equipos / energía eléctrica	22	10	32	2.7%	3.6%	2.0%	0.9%	3.0%
Medidas contra Phishing / Ingeniería Social	9	21	30	1.1%	7.6%	0.8%	1.9%	2.8%
Software de seguridad	15	11	26	1.9%	4.0%	1.4%	1.0%	2.4%
Hardware de seguridad	19	-	19	2.4%	-	1.8%	-	1.8%
Protección para garantizar la integridad personal y familiar	13	6	19	1.6%	2.2%	1.2%	0.6%	1.8%
Disponibilidad de la información	15	1	16	1.9%	0.4%	1.4%	0.1%	1.5%
No existe	5	11	16	0.6%	4.0%	0.5%	1.0%	1.5%
Garantía de continuidad en la operación	9	6	15	1.1%	2.2%	0.8%	0.6%	1.4%
Otros	10	7	17	1.2%	2.5%	0.9%	0.6%	1.6%
NS/NC	26	6	32	3.2%	2.2%	2.4%	0.6%	3.0%
	1309	397	1706					

GRÁFICA 4

Qué se entiende por Seguridad en Informática



A	Privacidad / Confidencialidad
B	Transmisión segura de datos
C	Medidas de seguridad en general (sin especificar)
D	Protección contra virus
E	Integridad / Confiabilidad de la información
F	Protección contra hackers
G	Acceso controlado
H	Protección contra spyware
I	Políticas adecuadas / procedimientos / uso responsable
J	Manejo de Identidad
K	Respaldo de información
L	Protección contra spam
M	Cuidado de los equipos / energía eléctrica
N	Medidas contra Phishing / Ingeniería Social
O	Software de seguridad

La principal percepción en general, tiene que ver con la privacidad y confidencialidad de la información. Los No Informáticos muestran una mayor preocupación por este rubro (ya que fue su mención con mayor frecuencia, mientras que para los Informáticos estuvo en el lugar número 8). Para el grupo de No Informáticos, su principal interés en este sentido giró alrededor de la privacidad y confidencialidad de su correo electrónico y de sus equipos en el trabajo.

En contraparte, los Informáticos tienen en mente, como principales conceptos de seguridad, aspectos como el Acceso Controlado, la Integridad y Confiabilidad de la información y la existencia de Políticas y Procedimientos.

Ambos grupos dan un lugar relevante a la Transmisión Segura de Datos (segundo lugar en frecuencia en los dos casos). Esto indica que las comunicaciones electrónicas se han incorporado a las prioridades de seguridad, incluso de los No Informáticos.

"Protección contra virus" como concepto aislado de recordación / identificación de seguridad en informática, bajó significativamente respecto de 2005, pasando de 30.5% al 17.0% de las menciones espontáneas de los entrevistados. Se denota una percepción más integral del problema como cuestión de la seguridad en las telecomunicaciones e integridad de la información, que los virus en sí mismos.

Es notoria una disminución considerable en la percepción de que la seguridad en informática no existe, respecto del estudio realizado en 2005, bajando de 6.1% a 1.5% de la muestra total (de 4.0% a 0.6 del grupo de los No Informáticos y del 10.8 a 4.0 del grupo de los Informáticos).

Aunque con una frecuencia reducida, resaltó que algunos entrevistados (1.8% de la muestra total) ven a la Seguridad en Informática como un medio necesario para proteger la integridad y seguridad personal y familiar.

Conceptos directamente relacionados con la productividad y rentabilidad de los negocios, como son Disponibilidad de la Información y la Garantía de Continuidad en la Operación, tuvieron muy pocas menciones (1.5% y 1.4% respectivamente).

Se percibe un mayor conocimiento sobre el software espía y sus consecuencias, en relación con el estudio anterior, principalmente entre los usuarios No Informáticos.

Asimismo, ha crecido la percepción de los correos no solicitados (Spam) como una posible amenaza contra la seguridad informática.

• Las mayores preocupaciones acerca de la Seguridad de equipos de cómputo y su contenido.

En las encuestas telefónicas se solicitó a los entrevistados que mencionaran las 3 principales amenazas que consideraban de manera espontánea. Posteriormente se les indicó que las numeraran de acuerdo al nivel de riesgo que percibían para cada una. En las encuestas por correo electrónico, se hizo la pregunta como se redacta a continuación:

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

a) La principal preocupación

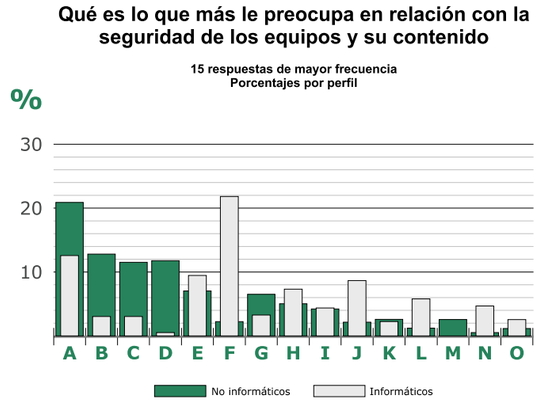
Este análisis corresponde a la respuesta número 1 de los entrevistados, considerada como la preocupación más importante. Ver Tabla 2 y Gráfica 5.

Tabla 2

La principal preocupación acerca de la Seguridad de equipos de cómputo y su contenido

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Virus	167	35	202	20.8%	12.6%	15.4%	3.2%	18.7%
Pérdida de la información	103	8	111	12.8%	2.9%	9.5%	0.7%	10.3%
Invasión a la privacidad	92	8	100	11.5%	2.9%	8.5%	0.7%	9.3%
Compras en línea / uso de banca electrónica	94	1	95	11.7%	0.4%	8.7%	0.1%	8.8%
Confidencialidad de la información	56	26	82	7.0%	9.4%	5.2%	2.4%	7.6%
Integridad de la información	18	61	79	2.2%	21.9%	1.7%	5.6%	7.3%
Robo de Identidad	52	9	61	6.5%	3.2%	4.8%	0.8%	5.6%
Hackers y otros agresores externos	40	20	60	5.0%	7.2%	3.7%	1.9%	5.6%
Extracción de información	34	12	46	4.2%	4.3%	3.1%	1.1%	4.3%
Spyware / Adware	17	24	41	2.1%	8.6%	1.6%	2.2%	3.8%
Software Deficiente	20	6	26	2.5%	2.2%	1.9%	0.6%	2.4%
Phishing / Ingeniería Social	9	16	25	1.1%	5.8%	0.8%	1.5%	2.3%
Spam	20	-	20	2.5%	-	1.9%	-	1.9%
Insuficiencia de infraestructura de seguridad (equipo/software)	4	13	17	0.5%	4.7%	0.4%	1.2%	1.6%
Desconocimiento	9	7	16	1.1%	2.5%	0.8%	0.6%	1.5%
Negligencia de usuarios	5	11	16	0.6%	4.0%	0.5%	1.0%	1.5%
Fallas de energía	11	4	15	1.4%	1.4%	1.0%	0.4%	1.4%
Pornografía / protección para menores	12	-	12	1.5%	-	1.1%	-	1.1%
Agresores internos	8	3	11	1.0%	1.1%	0.7%	0.3%	1.0%
Internet	7	3	10	0.9%	1.1%	0.6%	0.3%	0.9%
Otros	10	10	20	1.2%	3.6%	0.9%	0.9%	1.9%
NS/NC	15	1	16	1.9%	0.4%	1.4%	0.1%	1.5%
	803	278	1081					

Gráfica 5



A	Virus
B	Pérdida de la información
C	Invasión a la privacidad
D	Compras en línea / uso de banca electrónica
E	Confidencialidad de la información
F	Integridad de la información
G	Robo de Identidad
H	Hackers y otros agresores externos
I	Extracción de información
J	Spyware / Adware
K	Software Deficiente
L	Phishing / Ingeniería Social
M	Spam
N	Insuficiencia de infraestructura de seguridad (equipo/software)
O	Desconocimiento

Los virus siguen siendo la principal preocupación de las personas en general, como amenaza a la seguridad en informática (20.8% del grupo de los No Informáticos y 12.6% de los Informáticos). Sin embargo, resulta notorio que para este último grupo, los aspectos relacionados con la "Integridad de la información" como concepto global (21.9% de su grupo), son lo que más les preocupa, quedando los virus como su segunda mención.

También preocupa al usuario en general No Informático, la posibilidad de perder información (12.8% de este grupo) más que a los Informáticos (2.9%).

Llama la atención el aumento importante en la preocupación por la invasión a la privacidad. Denota que los usuarios están cada vez más conscientes del hecho de que la seguridad en informática está cada vez más ligada a elementos personales y que el comprometer los datos privados, tanto de una empresa como de una persona, es un riesgo sumamente importante.

Aparte de la Integridad de la información, aspectos como la confidencialidad, spyware, adware, phishing e ingeniería social, preocupan más a los Informáticos que a los No Informáticos.

Por su parte, para los No Informáticos también la seguridad ante el robo de identidad, resulta fundamental. En el estudio anterior, ningún miembro de este grupo lo mencionó como la amenaza de mayor riesgo, mientras en 2007 fue mencionado por el 6.5% de los No Informáticos entrevistados.

Respecto de los dos años anteriores, creció significativamente la preocupación por la seguridad en transacciones en línea y el uso de banca electrónica, principalmente entre el público en general No Informático (11.7%), quedando ésta en el lugar número 3 de este grupo.

b) Los 3 aspectos que, en conjunto, más preocupan

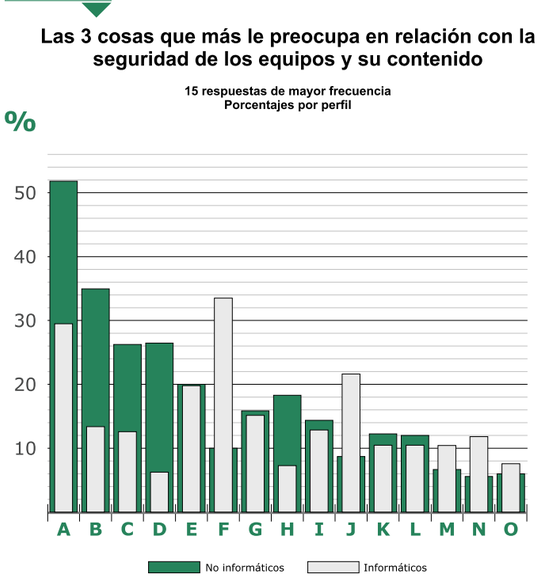
Corresponde a las 3 preocupaciones mencionadas por cada entrevistado (3,243 respuestas de 1,081 usuarios). En conjunto, las principales amenazas fueron como se describe en la Tabla 3 y en la Gráfica 6.

TABLA 3

Los 3 aspectos que, en conjunto, más preocupan acerca de la Seguridad de equipos de cómputo y su contenido

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Virus	417	82	499	51.9%	29.5%	38.6%	7.6%	46.2%
Pérdida de la información	280	37	317	34.9%	13.3%	25.9%	3.4%	29.3%
Invasión a la privacidad	210	35	245	26.2%	12.6%	19.4%	3.2%	22.7%
Compras en línea / uso de banca electrónica	212	17	229	26.4%	6.1%	19.6%	1.6%	21.2%
Confidencialidad de la información	161	55	216	20.0%	19.8%	14.9%	5.1%	20.0%
Integridad de la información	80	93	173	10.0%	33.5%	7.4%	8.6%	16.0%
Hackers y otros agresores externos	128	42	170	15.9%	15.1%	11.8%	3.9%	15.7%
Robo de Identidad	146	20	166	18.2%	7.2%	13.5%	1.9%	15.4%
Extracción de información	115	36	151	14.3%	12.9%	10.6%	3.3%	14.0%
Spyware / Adware	70	60	130	8.7%	21.6%	6.5%	5.6%	12.0%
Software Deficiente	98	29	127	12.2%	10.4%	9.1%	2.7%	11.7%
Spam	96	29	125	12.0%	10.4%	8.9%	2.7%	11.6%
Pornografía / protección para menores	55	29	84	6.8%	10.4%	5.1%	2.7%	7.8%
Phishing / Ingeniería Social	45	33	78	5.6%	11.9%	4.2%	3.1%	7.2%
Fallas de energía	48	21	69	6.0%	7.6%	4.4%	1.9%	6.4%
Desconocimiento	36	31	67	4.5%	11.2%	3.3%	2.9%	6.2%
Negligencia de usuarios	24	36	60	3.0%	12.9%	2.2%	3.3%	5.6%
Agresores internos	32	24	56	4.0%	8.6%	3.0%	2.2%	5.2%
Internet	28	20	48	3.5%	7.2%	2.6%	1.9%	4.4%
Insuficiencia de infraestructura de seguridad (equipo/software)	18	29	47	2.2%	10.4%	1.7%	2.7%	4.3%
Hardware Deficiente	22	17	39	2.7%	6.1%	2.0%	1.6%	3.6%
Nada / Ninguna	9	29	38	1.1%	10.4%	0.8%	2.7%	3.5%
Accesos Inalámbricos / Conectividad deficiente	13	15	28	1.6%	5.4%	1.2%	1.4%	2.6%
Daño a la productividad / a los resultados	4	6	10	0.5%	2.2%	0.4%	0.6%	0.9%
NS/NC	62	9	71	7.7%	3.2%	5.7%	0.8%	6.6%
	2409	834	3243					

GRÁFICA 6



A	Virus
B	Pérdida de la información
C	Invasión a la privacidad
D	Compras en línea / uso de banca electrónica
E	Confidencialidad de la información
F	Integridad de la información
G	Hackers y otros agresores externos
H	Robo de Identidad
I	Extracción de información
J	Spyware / Adware
K	Software Deficiente
L	Spam
M	Pornografía / protección para menores
N	Phishing / Ingeniería Social
O	Fallas de energía

Aunque la proporción de los datos representados de las 3 respuestas dadas en conjunto, es muy similar a la de las manifestadas como la preocupación mayor, si tomamos en cuenta las 3 menciones hechas por los entrevistados, vemos que hay algunas cuestiones que empiezan a tomar un peso significativo, como son el Spam (11.6% de todos los entrevistados), la pornografía por Internet y los filtros de contenido para protección de menores (7.8%).

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

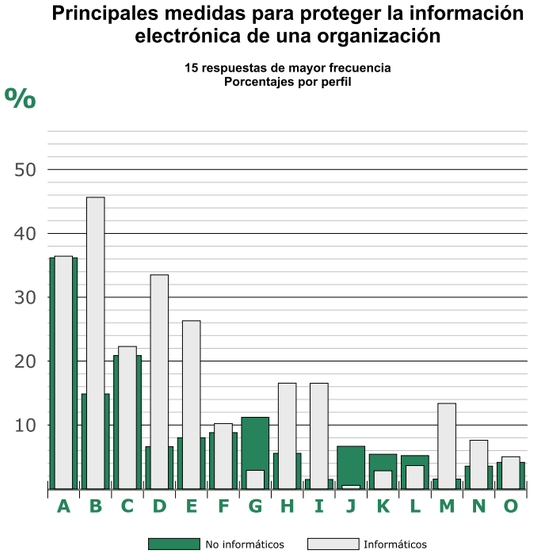
Pregunta: ¿Cuáles son las principales medidas que sugeriría para proteger la información electrónica de una organización?

TABLA 4

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

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Antivirus	290	101	391	36.1%	36.3%	26.8%	9.3%	36.2%
Firewalls / Proxy	120	127	247	14.9%	45.7%	11.1%	11.7%	22.8%
Controles de acceso y autenticación (Identidad - passwords - certificados digitales - tokens - biométricos)	168	62	230	20.9%	22.3%	15.5%	5.7%	21.3%
Políticas y procedimientos	53	93	146	6.6%	33.5%	4.9%	8.6%	13.5%
Respaldo de información	64	73	137	8.0%	26.3%	5.9%	6.8%	12.7%
Capacitación / Difusión / Concientización	70	28	98	8.7%	10.1%	6.5%	2.6%	9.1%
Medidas de seguridad en general (sin especificar)	89	8	97	11.1%	2.9%	8.2%	0.7%	9.0%
Encripción de datos / cifrado / encapsulado	45	46	91	5.6%	16.5%	4.2%	4.3%	8.4%
Implementación de controles físicos de acceso	11	46	57	1.4%	16.5%	1.0%	4.3%	5.3%
Software seguro / actualizado	54	1	55	6.7%	0.4%	5.0%	0.1%	5.1%
Anti-intrusos (IPS)	43	8	51	5.4%	2.9%	4.0%	0.7%	4.7%
Anti-spyware	41	10	51	5.1%	3.6%	3.8%	0.9%	4.7%
Monitoreo / administración eficiente de la red	14	37	51	1.7%	13.3%	1.3%	3.4%	4.7%
Administración centralizada	29	21	50	3.6%	7.6%	2.7%	1.9%	4.6%
Mejoras a la legislación	34	14	48	4.2%	5.0%	3.1%	1.3%	4.4%
Cultura de seguridad en informática	39	6	45	4.9%	2.2%	3.6%	0.6%	4.2%
Comunicación eficiente de políticas y procedimientos de seguridad	6	34	40	0.7%	12.2%	0.6%	3.1%	3.7%
Filtros de contenido para Internet	24	14	38	3.0%	5.0%	2.2%	1.3%	3.5%
Antispam	30	5	35	3.7%	1.8%	2.8%	0.5%	3.2%
Planes estructurados de seguridad (DRP, BCS…)	3	29	32	0.4%	10.4%	0.3%	2.7%	3.0%
Inversión mayor en Infraestructura de seguridad	16	14	30	2.0%	5.0%	1.5%	1.3%	2.8%
Sistemas Operativos más seguros / actualizados	1	29	30	0.1%	10.4%	0.1%	2.7%	2.8%
Análisis periódico de vulnerabilidades / estudio de seguridad	18	10	28	2.2%	3.6%	1.7%	0.9%	2.6%
Redundancia	3	24	27	0.4%	8.6%	0.3%	2.2%	2.5%
Vigilancia y supervisión	8	16	24	1.0%	5.8%	0.7%	1.5%	2.2%
Apoyo de Outsourcing (Consultores, Data Centers, hospedaje…)	20	3	23	2.5%	1.1%	1.9%	0.3%	2.1%
Implementación correcta de los sistemas	3	20	23	0.4%	7.2%	0.3%	1.9%	2.1%
Comunicaciones privadas (VPNs, VLANs...)	10	11	21	1.2%	4.0%	0.9%	1.0%	1.9%
Instalaciones físicas adecuadas	4	12	16	0.5%	4.3%	0.4%	1.1%	1.5%
Anti-phishing	11	4	15	1.4%	1.4%	1.0%	0.4%	1.4%
Protección accesos inalámbricos	2	13	15	0.2%	4.7%	0.2%	1.2%	1.4%
Reclutamiento y selección de personal adecuados	5	8	13	0.6%	2.9%	0.5%	0.7%	1.2%
Software legal / original	13	-	13	1.6%	-	1.2%	-	1.2%
Mantenimiento adecuado de instalaciones	1	10	11	0.1%	3.6%	0.1%	0.9%	1.0%
Cambiar de PC a Mac	2	8	10	0.2%	2.9%	0.2%	0.7%	0.9%
Mantenimiento adecuado de hardware	7	3	10	0.9%	1.1%	0.6%	0.3%	0.9%
Sistemas de administración de energía	5	5	10	0.6%	1.8%	0.5%	0.5%	0.9%
Otros	10	9	19	1.2%	3.2%	0.9%	0.8%	1.8%
NS/NC	98	7	105	12.2%	2.5%	9.1%	0.6%	9.7%
	1464	969	2433					

GRÁFICA 7



A	Antivirus
B	Firewalls / Proxy
C	Controles de acceso y autenticación
D	Políticas y procedimientos
E	Respaldo de información
F	Capacitación / Difusión / Concientización
G	Medidas de seguridad en general (sin especificar)
H	Encripción de datos / cifrado / encapsulado
I	Implementación de controles físicos de acceso
J	Software seguro / actualizado
K	Anti-intrusos (IPS)
L	Anti-spyware
M	Monitoreo / administración eficiente de la red
N	Administración centralizada
O	Mejoras a la legislación

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

El antivirus sigue siendo considerado como el mecanismo más importante para proteger los sistemas informáticos entre la muestra total, si bien el grupo de los Informáticos le dio prioridad al hecho de contar con algún dispositivo Firewall / Proxy.

Aunque las medidas principales para enfrentar los retos de seguridad en informática mencionadas, después del antivirus, siguen siendo firewalls y medidas de identificación de usuarios, llama poderosamente la atención que el 13.5% de todos los entrevistados mencionaron las políticas y procedimientos adecuados como uno de los aspectos primordiales y, entre usuarios que trabajan en áreas de informática, el 33.5% están conscientes de la importancia de este rubro.

En la gráfica, es claro cómo los Informáticos dan mayor relevancia a aspectos como Firewall / Proxy, Políticas, Procedimientos y Respaldo de Información.

Para ambos grupos, los controles de acceso y autenticación son muy importantes (lugar 3 en menciones del total de la muestra). La principal herramienta mencionada en este sentido, fue la utilización de contraseñas y preguntas secretas, tanto por los Informáticos como por los No Informáticos. Destacó un número significativo de menciones acerca de equipos biométricos y dispositivos con claves dinámicas, tipo token.

Se percibe asimismo una mayor conciencia y conocimiento acerca de soluciones contra intrusos, spyware, spam, etc. Los usuarios de ambos grupos demandan, de manera más enfática, que se hagan mejoras constantes en estos rubros.

Los servicios de Outsourcing aún no son vistos como una estrategia importante, en lo que se refiere a Seguridad en Informática, al ser mencionada únicamente por el 1.1% de los Informáticos.

En el estudio anterior, la capacitación ocupó el segundo lugar (con un 27.0%) después de Antivirus. Este año, bajó a la sexta posición con un 9.1%

• Elementos que son indispensables para tener redes inalámbricas seguras

Pregunta: ¿Cuáles considera que serían los elementos indispensables para tener redes inalámbricas seguras?

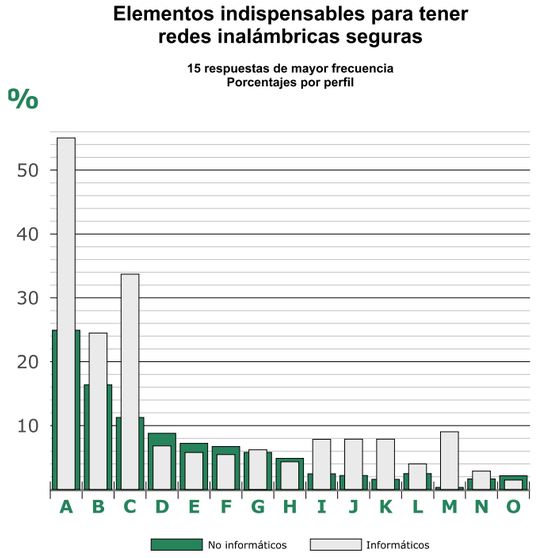
La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 5 y en la Gráfica 8.

TABLA 5

Elementos que son indispensables para tener redes inalámbricas seguras

	FRECUENCIA (fx) Actividad / Puesto			PORCENTAJES De su categoría		PORCENTAJES Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	**803**	**278**	**1,081**	**xni/803**	**xi/278**	**xni/1081**	**xi/1081**	
Controles de acceso y autenticación (Identidad - passwords - certificados digitales - tokens - biométricos)	200	153	**353**	24.9%	55.0%	18.5%	14.2%	**32.7%**
Utilizar antivirus, antispyware / antispam y firewalls	131	68	**199**	16.3%	24.5%	12.1%	6.3%	**18.4%**
Encripción de datos / cifrado / encapsulado	91	94	**185**	11.3%	33.8%	8.4%	8.7%	**17.1%**
Monitoreo / administración eficiente de la red	70	19	**89**	8.7%	6.8%	6.5%	1.8%	**8.2%**
Políticas y procedimientos	57	16	**73**	7.1%	5.8%	5.3%	1.5%	**6.8%**
Infraestructura adecuada	55	15	**70**	6.8%	5.4%	5.1%	1.4%	**6.5%**
Capacitación / Difusión / Concientización	47	17	**64**	5.9%	6.1%	4.3%	1.6%	**5.9%**
Buena señal / Buena conectividad	39	12	**51**	4.9%	4.3%	3.6%	1.1%	**4.7%**
Mayores penalizaciones legales	19	22	**41**	2.4%	7.9%	1.8%	2.0%	**3.8%**
Control por medio de identificación de tarjetas de red inalámbricas /MAC address	17	22	**39**	2.1%	7.9%	1.6%	2.0%	**3.6%**
Software / Sistema Operativo confiable	13	22	**35**	1.6%	7.9%	1.2%	2.0%	**3.2%**
Software legal / original / actualizado	20	11	**31**	2.5%	4.0%	1.9%	1.0%	**2.9%**
Usar antenas direccionales / acotar la señal	2	25	**27**	0.2%	9.0%	0.2%	2.3%	**2.5%**
Protocolos de comunicación seguros	13	8	**21**	1.6%	2.9%	1.2%	0.7%	**1.9%**
Sistemas IDS	17	4	**21**	2.1%	1.4%	1.6%	0.4%	**1.9%**
Control de empresas proveedoras de servicios	13	7	**20**	1.6%	2.5%	1.2%	0.6%	**1.9%**
Uso de VPN's /VLANS	5	15	**20**	0.6%	5.4%	0.5%	1.4%	**1.9%**
Control por IP	9	8	**17**	1.1%	2.9%	0.8%	0.7%	**1.6%**
Crear redes / zonas distintas para diferentes usos	13	4	**17**	1.6%	1.4%	1.2%	0.4%	**1.6%**
No se puede	12	4	**16**	1.5%	1.4%	1.1%	0.4%	**1.5%**
Otros	14	14	**28**	1.7%	5.0%	1.3%	1.3%	**2.6%**
NS/NC	218	11	**229**	27.1%	4.0%	20.2%	1.0%	**21.2%**
	1075	**571**	**1646**					

GRÁFICA 8



A	Controles de acceso y autenticación
B	Utilizar antivirus, antispyware / antispam y firewalls
C	Encripción de datos / cifrado / encapsulado
D	Monitoreo / administración eficiente de la red
E	Políticas y procedimientos
F	Infraestructura adecuada
G	Capacitación / Difusión / Concientización
H	Buena señal / Buena conectividad
I	Mayores penalizaciones legales
J	Control por medio de identificación de tarjetas de red inalámbricas /MAC address
K	Software / Sistema Operativo confiable
L	Software legal / original / actualizado
M	Usar antenas direccionales / acotar la señal
N	Protocolos de comunicación seguros
O	Sistemas IDS

JFS

Si bien el número de respuestas por persona entrevistada es mayor por parte de los Informáticos que de los No Informáticos en este rubro, destaca una alta participación de este último grupo (73% de los No Informáticos dieron alguna respuesta) con sugerencias al respecto. Inclusive, sorprende que una mayor proporción de No Informáticos propuso soluciones relacionadas con el monitoreo y administración eficiente de la red, políticas y procedimientos e infraestructura adecuada, respecto de los Informáticos.

Los rubros considerados por los entrevistados como más importantes para esta función, fueron controles de acceso y autenticación (32.7% de la muestra total), utilización de herramientas como antivirus, firewalls, antispyware y antispam (18.4%), y la encripción de datos (17.1%).

- **Elementos que son indispensables para comprobar la identidad de manera electrónica**

Pregunta: ¿Cuáles considera que serían los elementos indispensables para comprobar, de forma electrónica, su identidad como usuario?

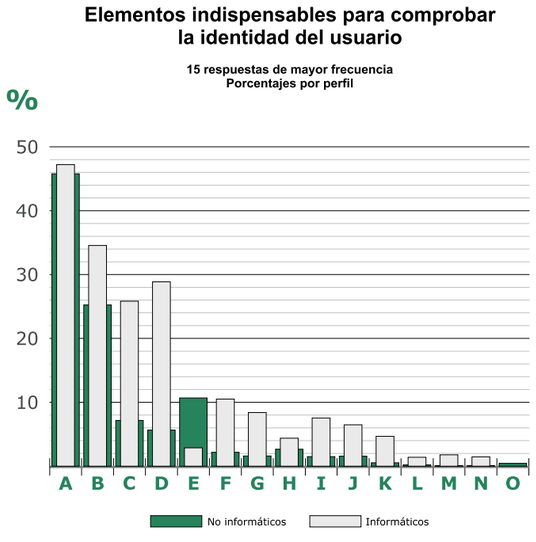
La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 6 y en la Gráfica 9.

TABLA 5

Elementos que son indispensables para comprobar la identidad de manera electrónica

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
User ID / Contraseña	368	131	499	45.8%	47.1%	34.0%	12.1%	46.2%
Biométricos	202	96	298	25.2%	34.5%	18.7%	8.9%	27.6%
Certificados / Firma electrónica	57	72	129	7.1%	25.9%	5.3%	6.7%	11.9%
Token / Clave dinámica SMS o e-mail	46	80	126	5.7%	28.8%	4.3%	7.4%	11.7%
Preguntas clave	86	8	94	10.7%	2.9%	8.0%	0.7%	8.7%
Gafete / tarjeta ID	18	29	47	2.2%	10.4%	1.7%	2.7%	4.3%
Administración centralizada	14	23	37	1.7%	8.3%	1.3%	2.1%	3.4%
ID del equipo (Mac address / nombre del equipo)	22	12	34	2.7%	4.3%	2.0%	1.1%	3.1%
Dirección IP	12	21	33	1.5%	7.6%	1.1%	1.9%	3.1%
Encripción de datos	14	18	32	1.7%	6.5%	1.3%	1.7%	3.0%
Cámaras en los equipos	3	13	16	0.4%	4.7%	0.3%	1.2%	1.5%
Patrones	2	4	6	0.2%	1.4%	0.2%	0.4%	0.6%
Seguimiento de políticas	1	5	6	0.1%	1.8%	0.1%	0.5%	0.6%
Tarjeta de claves irrepetibles	1	4	5	0.1%	1.4%	0.1%	0.4%	0.5%
Ninguno	3	-	3	0.4%	-	0.3%	-	0.3%
Verificación caligráfica	1	-	1	0.1%	-	0.1%	-	0.1%
NS/NC	219	10	229	27.3%	3.6%	20.3%	0.9%	21.2%
	1069	**526**	**1595**					

GRÁFICA 9



A	User ID / Contraseña
B	Biométricos
C	Certificados / Firma electrónica
D	Token / Clave dinámica SMS o e-mail
E	Preguntas clave
F	Gafete / tarjeta ID
G	Administración centralizada
H	ID del equipo (Mac address / nombre del equipo)
I	Dirección IP
J	Encripción de datos
K	Cámaras en los equipos
L	Patrones
M	Seguimiento de políticas
N	Tarjeta de claves irrepetibles
O	Ninguno

El elemento de comprobación de identidad más identificado por los entrevistados, fue el uso de claves y contraseñas, con el 46.2% de las menciones totales.

Hablando específicamente de mecanismos para el manejo de identidad, fue interesante ver que muchos usuarios (27.6%) mencionaron algún tipo de biométrico (huella digital, reconocimiento de iris, reconocimiento de voz, etc.) Aunque el uso de claves y contraseñas fue el rubro más mencionado, es claro que los usuarios están percibiendo las posibilidades de los dispositivos biométricos y su lugar dentro del mundo de seguridad en informática.

7.1% de los entrevistados No Informáticos (y 25.9% de los Informáticos), mencionaron los certificados digitales o firma electrónica como un elemento necesario de comprobación de identidad (11.9% de la muestra total).

Las claves dinámicas, como son los tokens y las confirmaciones enviadas vía correo electrónico o mensaje de texto a teléfono celular (SMS), fueron una de las alternativas más mencionadas por ambos grupos (11.7% de la muestra total).
Aunque con una frecuencia menor, fueron mencionadas otras opciones de autenticación, como las preguntas clave, los gafetes y tarjetas de identidad, entre las que se encontraron tarjetas de proximidad, chip, cinta magnética, etc., y otros recursos lógicos, como contar con una administración centralizada, MAC address, dirección IP y datos encriptados, entre otros.

• Normas y regulaciones de seguridad que conoce

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

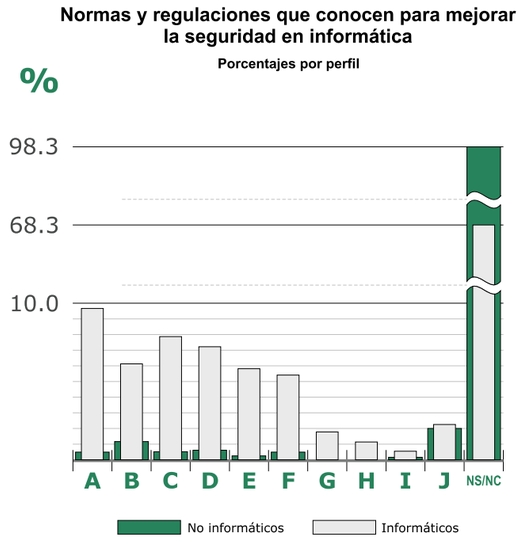
La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 7 y en la Gráfica 10.

TABLA 7

Normas y regulaciones de seguridad que conoce

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
ISO 17799	3	27	30	0.4%	9.7%	0.3%	2.5%	2.8%
ISO/IEC	9	17	26	1.1%	6.1%	0.8%	1.6%	2.4%
Sarbanes-Oxley	4	22	26	0.5%	7.9%	0.4%	2.0%	2.4%
CISSP	5	20	25	0.6%	7.2%	0.5%	1.9%	2.3%
ISO 27001	2	16	18	0.2%	5.8%	0.2%	1.5%	1.7%
SISA	3	15	18	0.4%	5.4%	0.3%	1.4%	1.7%
CSA	-	5	5	-	1.8%	-	0.5%	0.5%
FISMA	-	3	3	-	1.1%	-	0.3%	0.3%
BS 7799-2	1	1	2	0.1%	0.4%	0.1%	0.1%	0.2%
ANSI	1	-	1	0.1%	-	0.1%	-	0.1%
BICSI	1	-	1	0.1%	-	0.1%	-	0.1%
British Standards	1	-	1	0.1%	-	0.1%	-	0.1%
CMMI	1	-	1	0.1%	-	0.1%	-	0.1%
CobIT Risk Management	1	-	1	0.1%	-	0.1%	-	0.1%
FCC	1	-	1	0.1%	-	0.1%	-	0.1%
FIPS 197	1	-	1	0.1%	-	0.1%	-	0.1%
IEEE	1	-	1	0.1%	-	0.1%	-	0.1%
IEEE 694	1	-	1	0.1%	-	0.1%	-	0.1%
IEEE 802.11 i	1	-	1	0.1%	-	0.1%	-	0.1%
IMPI	1	-	1	0.1%	-	0.1%	-	0.1%
ITIL	-	1	1	-	0.4%	-	0.1%	0.1%
ITSP&P	-	1	1	-	0.4%	-	0.1%	0.1%
JTC1	-	1	1	-	0.4%	-	0.1%	0.1%
Ley de medios electrónicos del Estado de Guanajuato	1	-	1	0.1%	-	0.1%	-	0.1%
Libro Naranja	-	1	1	-	0.4%	-	0.1%	0.1%
Normas de Condusef	1	-	1	0.1%	-	0.1%	-	0.1%
Normas de la Comisión Nacional Bancaria	1	-	1	0.1%	-	0.1%	-	0.1%
Normas de la SHCP	1	-	1	0.1%	-	0.1%	-	0.1%
OPSEC	1	-	1	0.1%	-	0.1%	-	0.1%
RSA	-	1	1	-	0.4%	-	0.1%	0.1%
SLP	-	1	1	-	0.4%	-	0.1%	0.1%
NS/ NC	789	190	979	98.3%	68.3%	73.0%	17.6%	90.6%
	832	322	1154					

GRÁFICA 10



A	ISO 17799
B	ISO/IEC
C	Sarbanes-Oxley
D	CISSP
E	ISO 27001
F	SISA
G	CSA
H	FISMA
I	BS 7799-2
J	Otras
NS/NC	No sabe / No contestó

Existe un alto grado de desconocimiento de las normas y regulaciones relacionadas con seguridad en informática. De hecho, el 90.6% de todos los usuarios de la muestra total (tanto Informáticos como No Informáticos) y el 68.3% de usuarios que trabajan en áreas de informática (Informáticos), no pudieron mencionar ninguna de ellas. Sólo 14 de 803 No Informáticos (1.7%) mencionaron una o varias de ellas.

Las normas mejor identificadas por los Informáticos que mencionaron alguna, mencionadas por más del 5% de este grupo, fueron ISO 17799, Sarbanes-Oxley, CISSP, ISO/IEC, SISA e ISO 27001.

La norma mejor identificada por los No Informáticos (sólo por 9 de los entrevistados), fue la ISO/IEC.

• Percepción acerca de diversas marcas asociadas con Seguridad en Informática

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

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

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

Las respuestas clasificadas a ambas preguntas, pueden consultarse en las respectivas Tabla 8 y Tabla 9.

TABLA 8

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

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Symantec / Norton / Veritas	194	70	264	24.2%	25.2%	17.9%	6.5%	24.4%
Cisco	55	98	153	6.8%	35.3%	5.1%	9.1%	14.2%
McAfee	98	15	113	12.2%	5.4%	9.1%	1.4%	10.5%
HP	67	35	102	8.3%	12.6%	6.2%	3.2%	9.4%
Panda	66	20	86	8.2%	7.2%	6.1%	1.9%	8.0%
Microsoft	61	11	72	7.6%	4.0%	5.6%	1.0%	6.7%
Linux	34	28	62	4.2%	10.1%	3.1%	2.6%	5.7%
Ninguna	34	22	56	4.2%	7.9%	3.1%	2.0%	5.2%
Apple / Macintosh	36	19	55	4.5%	6.8%	3.3%	1.8%	5.1%
3Com	23	23	46	2.9%	8.3%	2.1%	2.1%	4.3%
Dell	34	12	46	4.2%	4.3%	3.1%	1.1%	4.3%
Checkpoint	18	24	42	2.2%	8.6%	1.7%	2.2%	3.9%
Pc cillin	25	15	40	3.1%	5.4%	2.3%	1.4%	3.7%
Firefox	12	21	33	1.5%	7.6%	1.1%	1.9%	3.1%
Kaspersky	12	21	33	1.5%	7.6%	1.1%	1.9%	3.1%
Windows	12	19	31	1.5%	6.8%	1.1%	1.8%	2.9%
Juniper	11	19	30	1.4%	6.8%	1.0%	1.8%	2.8%
Nod32	7	18	25	0.9%	6.5%	0.6%	1.7%	2.3%
IBM	13	10	23	1.6%	3.6%	1.2%	0.9%	2.1%
Oracle	7	16	23	0.9%	5.8%	0.6%	1.5%	2.1%
Sony	21	1	22	2.6%	0.4%	1.9%	0.1%	2.0%
Windows XP	15	7	22	1.9%	2.5%	1.4%	0.6%	2.0%
Avg	13	8	21	1.6%	2.9%	1.2%	0.7%	1.9%
Citrix	5	15	20	0.6%	5.4%	0.5%	1.4%	1.9%
Computer Associates	8	12	20	1.0%	4.3%	0.7%	1.1%	1.9%
Hauri	8	12	20	1.0%	4.3%	0.7%	1.1%	1.9%
VeriSign	4	16	20	0.5%	5.8%	0.4%	1.5%	1.9%
Intel	8	11	19	1.0%	4.0%	0.7%	1.0%	1.8%
Tipping Point	8	9	17	1.0%	3.2%	0.7%	0.8%	1.6%
Ad-aware	8	6	14	1.0%	2.2%	0.7%	0.6%	1.3%
Gateway	7	7	14	0.9%	2.5%	0.6%	0.6%	1.3%
EMC2	4	9	13	0.5%	3.2%	0.4%	0.8%	1.2%
Sonicwall	2	11	13	0.2%	4.0%	0.2%	1.0%	1.2%
Sun	4	8	12	0.5%	2.9%	0.4%	0.7%	1.1%
Toshiba	12	-	12	1.5%	-	1.1%	-	1.1%
RSA Security	4	6	10	0.5%	2.2%	0.4%	0.6%	0.9%
Trend Micro	6	4	10	0.7%	1.4%	0.6%	0.4%	0.9%
Avasat	3	6	9	0.4%	2.2%	0.3%	0.6%	0.8%
Avaya	2	7	9	0.2%	2.5%	0.2%	0.6%	0.8%
Nokia	-	9	9	-	3.2%	-	0.8%	0.8%
Otras	83	48	131	10.3%	17.3%	7.7%	4.4%	12.1%
NS/NC	354	77	431	44.1%	27.7%	32.7%	7.1%	39.9%
	1398	805	2203					

TABLA 9

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

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Microsoft	66	36	102	8.2%	12.9%	6.1%	3.3%	9.4%
Symantec / Norton / Veritas	47	50	97	5.9%	18.0%	4.3%	4.6%	9.0%
Todas	46	31	77	5.7%	11.2%	4.3%	2.9%	7.1%
Windows	32	21	53	4.0%	7.6%	3.0%	1.9%	4.9%
Panda	20	18	38	2.5%	6.5%	1.9%	1.7%	3.5%
McAfee	26	11	37	3.2%	4.0%	2.4%	1.0%	3.4%
HP	15	9	24	1.9%	3.2%	1.4%	0.8%	2.2%
Dell	5	17	22	0.6%	6.1%	0.5%	1.6%	2.0%
IBM	10	6	16	1.2%	2.2%	0.9%	0.6%	1.5%
Internet Explorer	6	9	15	0.7%	3.2%	0.6%	0.8%	1.4%
Intel	8	3	11	1.0%	1.1%	0.7%	0.3%	1.0%
Pc cillin	6	5	11	0.7%	1.8%	0.6%	0.5%	1.0%
Windows XP	8	2	10	1.0%	0.7%	0.7%	0.2%	0.9%
Acer	9	-	9	1.1%	-	0.8%	-	0.8%
Otras	65	37	102	8.1%	13.3%	6.0%	3.4%	9.4%
NS/NC	456	163	619	56.8%	58.6%	42.2%	15.1%	57.3%
	825	418	1243					

• Qué hace falta por parte de los proveedores de TI

Pregunta: En materia de Seguridad en Informática, ¿qué cree que haga falta por parte de los proveedores de tecnología?

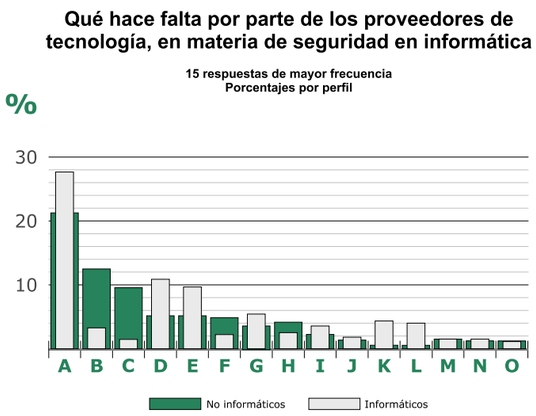
La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 10 y en la Gráfica 11.

TABLA 10

Qué hace falta por parte de los proveedores de TI

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Mayor difusión / divulgación / concientización	170	77	247	21.2%	27.7%	15.7%	7.1%	22.8%
Más / mejores herramientas en general	100	9	109	12.5%	3.2%	9.3%	0.8%	10.1%
Precios más accesibles	77	4	81	9.6%	1.4%	7.1%	0.4%	7.5%
Compromiso / honestidad con los usuarios	42	30	72	5.2%	10.8%	3.9%	2.8%	6.7%
Capacitación para usuarios	42	27	69	5.2%	9.7%	3.9%	2.5%	6.4%
Actualización / Vanguardia en el desarrollo de sus productos	39	6	45	4.9%	2.2%	3.6%	0.6%	4.2%
Información más accesible para personas no especializadas	29	15	44	3.6%	5.4%	2.7%	1.4%	4.1%
Mejoras en el software / actualizaciones	33	7	40	4.1%	2.5%	3.1%	0.6%	3.7%
Métodos mejores de manejo de identidad	17	10	27	2.1%	3.6%	1.6%	0.9%	2.5%
Involucramiento con las necesidades reales del cliente	11	5	16	1.4%	1.8%	1.0%	0.5%	1.5%
Mayor capacidad técnica / conocimientos de los proveedores	4	12	16	0.5%	4.3%	0.4%	1.1%	1.5%
Calidad	4	11	15	0.5%	4.0%	0.4%	1.0%	1.4%
Mejores soluciones para la Privacidad	11	4	15	1.4%	1.4%	1.0%	0.4%	1.4%
Mejor soporte técnico	10	4	14	1.2%	1.4%	0.9%	0.4%	1.3%
Mejores soluciones contra hackers	10	3	13	1.2%	1.1%	0.9%	0.3%	1.2%
Productos integrados, que desde su origen sean seguros	10	3	13	1.2%	1.1%	0.9%	0.3%	1.2%
Mayor asesoría / consultoría	-	12	12	-	4.3%	-	1.1%	1.1%
Mejor evaluación de sus productos antes de liberarlos	10	-	10	1.2%	-	0.9%	-	0.9%
Otros	41	25	66	5.1%	9.0%	3.8%	2.3%	6.1%
NS/NC	232	26	258	28.9%	9.4%	21.5%	2.4%	23.9%
	892	290	1182					

GRÁFICA 11



A	Mayor difusión / divulgación / concientización
B	Más / mejores herramientas en general
C	Precios más accesibles
D	Compromiso / honestidad con los usuarios
E	Capacitación para usuarios
F	Actualización / Vanguardia en el desarrollo de sus productos
G	Información más accesible para personas no especializadas
H	Mejoras en el software / actualizaciones
I	Métodos mejores de manejo de identidad
J	Involucramiento con las necesidades reales del cliente
K	Mayor capacidad técnica / conocimientos de los proveedores
L	Calidad
M	Mejores soluciones para la Privacidad
N	Mejor soporte técnico
O	Mejores soluciones contra hackers

JFS

Tanto los usuarios Informáticos como los No Informáticos, demandan una mayor difusión y divulgación de contenidos de seguridad (22.8% de la muestra total). En este sentido, destaca la solicitud de los usuarios de ambos grupos para que la información proporcionada por los proveedores de tecnología, sea más fácil de entender, de tal manera que personas no especializadas tengan elementos para seguir prácticas seguras en el desempeño de su trabajo.

Después de una mayor difusión, los usuarios Informáticos mencionaron requerir más y mejores herramientas en general, así como precios más accesibles. Comentaron que el software y los equipos deberían salir de la fábrica siendo soluciones seguras en sí mismas, con los mayores alcances posibles, así como tener características estandarizadas que les permitan integrarse con otras marcas fácilmente. También enfatizaron que los proveedores de tecnología deben fabricar y distribuir productos vanguardistas, que se adelanten lo más posible a los problemas de inseguridad que constantemente están surgiendo.

Por su parte, los usuarios No Informáticos perciben deficiencias en cuanto a la honestidad de los proveedores para proponerles soluciones y en cuanto al compromiso que deberían tener con sus necesidades tanto técnicas como presupuestales.

Mayor capacitación para los usuarios vuelve a estar entre los rubros más demandados por ambos grupos, tanto No Informáticos como Informáticos.

Otros aspectos importantes demandados por el grupo de No Informáticos, fueron un mayor apoyo por parte de consultores bien capacitados y con estándares de calidad de servicio bien definidos.

- **Qué más les gustaría conocer acerca de Seguridad en Informática**

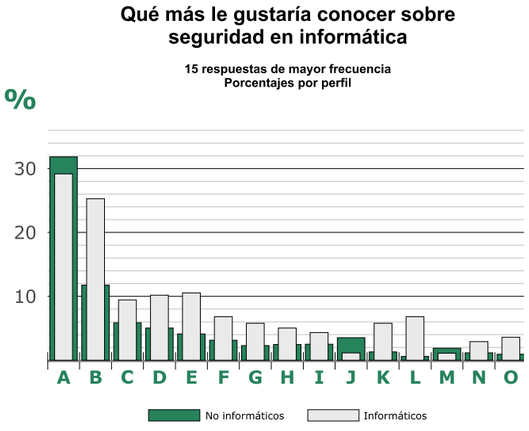
Ver tabla de frecuencias y gráfica de respuestas en la Tabla 11 y en la Gráfica 12.

TABLA 11

Que más les gustaria conocer acerca de Seguridad en Informatica

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Muestra =	803	278	1,081	xni/803	xi/278	xni/1081	xi/1081	
Seguridad en Informática en general / todo	255	81	336	31.8%	29.1%	23.6%	7.5%	31.1%
Avances / tendencias / actualizaciones	95	70	165	11.8%	25.2%	8.8%	6.5%	15.3%
Costo-Beneficio de los diferentes productos y servicios ofertados.	47	26	73	5.9%	9.4%	4.3%	2.4%	6.8%
Políticas y procedimientos / Mejores Prácticas a nivel mundial	40	28	68	5.0%	10.1%	3.7%	2.6%	6.3%
Regulación / Normatividad / Legislación	33	29	62	4.1%	10.4%	3.1%	2.7%	5.7%
Hardware y software	25	19	44	3.1%	6.8%	2.3%	1.8%	4.1%
Tecnología inalámbrica	18	16	34	2.2%	5.8%	1.7%	1.5%	3.1%
Más acerca de virus	19	14	33	2.4%	5.0%	1.8%	1.3%	3.1%
Seguridad en Internet	20	12	32	2.5%	4.3%	1.9%	1.1%	3.0%
Información de riesgos	28	3	31	3.5%	1.1%	2.6%	0.3%	2.9%
Manejo de Identidad	10	16	26	1.2%	5.8%	0.9%	1.5%	2.4%
Monitoreo y administración de redes	5	19	24	0.6%	6.8%	0.5%	1.8%	2.2%
Más acerca de Hackers	15	3	18	1.9%	1.1%	1.4%	0.3%	1.7%
Combate contra Spam	9	8	17	1.1%	2.9%	0.8%	0.7%	1.6%
Más acerca de Firewalls	7	10	17	0.9%	3.6%	0.6%	0.9%	1.6%
Seguridad en Comercio Electrónico	8	9	17	1.0%	3.2%	0.7%	0.8%	1.6%
Seguridad en telecomunicaciones	9	8	17	1.1%	2.9%	0.8%	0.7%	1.6%
Combate contra Spyware / Adware	12	4	16	1.5%	1.4%	1.1%	0.4%	1.5%
Información sobre las empresas de seguridad en informática	14	1	15	1.7%	0.4%	1.3%	0.1%	1.4%
Otros	17	30	47	2.1%	10.8%	1.6%	2.8%	4.3%
NS/NC	157	15	172	19.6%	5.4%	14.5%	1.4%	15.9%
	843	421	1264					

GRÁFICA 12



A	Seguridad en Informática en general / todo
B	Avances / tendencias / actualizaciones
C	Costo-Beneficio de los diferentes productos y servicios ofertados.
D	Políticas y procedimientos / Mejores Prácticas a nivel mundial
E	Regulación / Normatividad / Legislación
F	Hardware y software
G	Tecnología inalámbrica
H	Más acerca de virus
I	Seguridad en Internet
J	Información de riesgos
K	Manejo de Identidad
L	Monitoreo y administración de redes
M	Más acerca de Hackers
N	Combate contra Spam
O	Más acerca de Firewalls

Los usuarios quieren más información veraz, de cualquier fuente. El 31.1% de los entrevistados mencionó que les gustaría conocer más acerca de todos los aspectos de seguridad y el 15.3% especificó que le gustaría estar al tanto de novedades y actualizaciones en el tema.

El 6.3% mencionó que le gustaría saber más acerca de políticas y procedimientos, así como mejores prácticas a nivel mundial. Comparando con años anteriores, es un avance importante, e indica que la cultura en seguridad en informática está aumentando en nuestro país.

Asimismo, haciendo un análisis comparativo con los resultados de los dos estudios anteriores, se percibe que un porcentaje significativo de los entrevistados (5.7% de la muestra total), mostró interés por temas relacionados con la normatividad y legislación en la materia, contra una frecuencia menor al 0.7% en el estudio de 2005.

Resulta notorio que los virus en sí, a pesar de ser una de las principales preocupaciones como amenaza para la seguridad en informática, no forman parte de los aspectos en los que los usuarios pretendan profundizar. En el estudio anterior, 14.3% mencionó que le gustaría conocer más acerca de virus, contra un 3.1% de la muestra total de este estudio. Conocer más acerca de Hackers, pasó de ocupar la 3ª posición en el estudio anterior (14.0%) a la posición 13 (1.7%) en el estudio 2007.

JFS

III. ESTUDIO CON ESPERTOS 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
3Com	Ignacio Leñero	Director General
Andresen y Asociados Consultores	Carlos Carranza A.	Director General
Asiste	Moisés Polishuk	Director General
Banorte	Salvador Sierra Hernández	Director de Soporte Técnico e Infraestructura
Board Media	Dan Ostrosky Shejet	Consultor independiente y consejero de varias empresas
CA Software de México	Jorge Plascencia Zurita	Business Technologist
Cablevisión	Israel Madiedo Luna	Director de Sistemas de Red
Citrix Sistemas de México	Miranda Hernández Landavazo	Gerente de Mercadotecnia
Fundación Ealy Ortiz, A.C.	Enrique Bustamante Martínez	Director General
Infosinergia	Alejandro Romay Muñoz de Cote	Director General
ITESM Campus Estado de México	Francisco Camargo	Director de Informática
Jonima	Nils Olryd	Director General
Kio Networks	Diego F. Lastra S.	Chief Information Security Officer
Mattica	Andrés Velázquez	Director de Investigaciones Digitales
Mexis, Seguridad Administrada	Antonio Llausás Zamarripa Jorge J. Díaz Denis	Director Comercial y de Alianzas Director de Desarrollo de Productos y Mercadotecnia
QoS Labs de México	Iván Santacruz Ortiz	Director de Mercadotecnia
Siemens	Arturo Olguín Alpízar	CIO Mesoamérica

RESULTADOS

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

Se reconoce que la Seguridad en Informática está en pleno desarrollo en nuestro país, con avances notables en diversos renglones, principalmente entre los corporativos, las empresas transnacionales y empresas grandes. Sin embargo, el consenso es que existe aún un rezago importante en este rubro a nivel país, principalmente por motivos como los que se describen:

- El nivel es equiparable, e incluso superior, con el de otros países de América Latina, pero muy inferior comparando con países desarrollados.
- Estamos lejos de ser un país culto en materia de Seguridad en Informática. Se requiere mucho más difusión y concientización al respecto, tanto a nivel empresarial como personal.
- Falta madurez en las empresas, para incorporar a la seguridad de la información como parte de sus procesos y de sus decisiones estratégicas.
- No se invierte lo suficiente en este rubro, lo que provoca que la infraestructura tecnológica, en general, sea insuficiente.
- México es un país débil en el ámbito regulatorio.
- Se tienen índices muy altos de piratería.

Los puntos de vista más positivos, reconocen que se está en un nivel competitivo en diversos rubros, como es el caso de las instituciones financieras para el manejo de banca electrónica, pero hace falta mucho por hacer, sobre todo a nivel de las PyMEs y de educación en general.

Se considera que existen conocimientos y experiencia desarrollados en el país, que se desperdician, sin embargo, por la poca implementación que se lleva a cabo.

OBSERVACIONES MÁS RELEVANTES

"México se encuentra justo en el medio de un importante cambio en el desarrollo tecnológico de la Seguridad Informática. A pesar de que estamos lejos de estar a la vanguardia, debido a que no generemos infraestructura tecnológica, tampoco estamos en último lugar, ya que utilizamos y diseñamos tecnología de seguridad informática de primer nivel".

"En pleno desarrollo, con mejoras en la legislación y la cultura de seguridad, con los usuarios tomando mayor conciencia de la situación y cuidado de la misma".

"México presenta grandes avances en las Instituciones Financieras (Bancos, Casas de Bolsa, etc.), como es de esperarse, ya que al manejar dinero y tener los recursos, se han preocupado por integrar tecnología de punta en el manejo de la seguridad.

"En el caso de la Industria en General, son los grandes corporativos los que se han preocupado por invertir en este rubro, aunque en algunos casos lo han hecho de manera un tanto equivocada, ya que han enfocado sus baterías al control de los usuarios, sin integrar políticas claras para evitar daños trascendentes como, por ejemplo, el espionaje industrial".

"Está empezando a hacerse conciente de los problemas que enfrenta en seguridad. Las empresas en México empiezan ya a implementar políticas y estrategias tanto para asegurar la información como para bloquear accesos o uso inválido de su infraestructura. Todavía no estamos suficientemente culturizados en México para hacer de la seguridad en informática una práctica habitual, pero definitivamente vamos hacia allá".

"México está en una posición muy ventajosa con respecto al mundo, la cual lamentablemente no se está explotando. Por un lado, vemos cómo funciona la tecnología que está siendo utilizada en todo el mundo antes de incorporarla en México.

"Consideramos que México está un poco rezagado en la implementación de la tecnología, mas no en conocimientos y experiencia que se puede encontrar en los especialistas en el tema".

"Es quizás en otros giros en donde, como consecuencia de que no se han podido justificar presupuestos para seguridad en informática, ésta es pobre respecto de mismos giros en el resto del mundo".

"'Verde' (inmaduro), no hay una madurez en las empresas para entender el verdadero alcance de una estrategia de seguridad, en nuestra experiencia, las empresas en México, principalmente aquéllas que toman las decisiones de compra de tecnología de forma local, aún siguen preocupados por componentes como lo son el anti-virus, anti-spam y el firewall como principales medidas de seguridad.

"México se encuentra en un proceso de adopción y entendimiento en materia de seguridad, si bien estamos muy cerca de EU el nivel de conocimiento de los riesgos es muy bajo y por otra parte, la capacidad de acceder a las tecnologías en cuestión de costo, implementación, certificación todavía no justifican su inversión en los presupuestos de las empresas mexicanas.

"Uno de los principales motores para la adopción de tecnologías en Seguridad Informática en los EU ha sido las regulaciones en las diferentes ramas de la industria, mayormente en la financiera y salud, sin embargo, en México existe una brecha regulatoria en materia de información".

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

Las respuestas codificadas de todos los entrevistados (quienes dieron, en la mayoría de los casos, más de una opinión cada uno), giraron alrededor de once rubros principalmente, como puede observarse en la Gráfica 13.

GRÁFICA 13

Principales retos de México en materia de Seguridad en Informática

Los expertos perciben como reto principal, el realizar mayores esfuerzos por inculcar la Seguridad en Informática entre todos los usuarios, tanto a nivel personal como empresarial. Los usuarios deben estar conscientes de los riesgos que existen para no incurrir en pérdidas de productividad o incluso de un valioso capital, como es la información, los secretos industriales, etc. Entre otras perspectivas, se manifestó la necesidad de que las personas reconozcan que la Seguridad en Informática no es únicamente una cuestión de tecnología, sino de procesos y buenas prácticas. Esta responsabilidad recae en todos los actores que tienen relación con el tema, principalmente de las empresas proveedoras de tecnología y las instituciones educativas, quienes pueden y deben reforzar las actividades de difusión y capacitación, entre otras.

Una de las principales preocupaciones de los entrevistados, es la falta de leyes claras que permitan delimitar los delitos electrónicos y sancionar de manera efectiva a quienes incurren en ellos. Ambos aspectos (la promoción de una cultura de seguridad entre los usuarios y la regulación adecuada sobre los recursos tecnológicos y su uso), entre otras cosas, deben dar mayor certidumbre a las empresas desarrolladoras de soluciones y atacar la piratería de una manera más contundente.

Entre los retos más mencionados por los expertos, estuvieron la calidad de los productos ofrecidos (principalmente de aquéllos desarrollados en el país) y de los servicios que brindan fabricantes, canales de distribución, consultores, desarrolladores, etc., así como del precio, en donde se demanda más apoyo para que las empresas medianas y pequeñas puedan tener acceso a aplicaciones seguras.

Estar al día en materia de Seguridad en Informática, es también algo en lo que las personas especializadas deben poner atención. Se percibe que existen algunos huecos en cuanto a los niveles de actualización de conocimientos sobre las nuevas tecnologías por parte de algunos proveedores de tecnología.

OBSERVACIONES MÁS **RELEVANTES**

"Difusión y masificación de la cultura de Seguridad Informática, como un factor indispensable para la competitividad y el desarrollo del País".

"Generar la cultura de la seguridad en el publico en general, ya que en los hogares y en las escuelas es en donde es mínima o nula la preocupación y conocimiento de estos temas".

"El primer reto es el tomar conciencia del enorme potencial que representa la alineación de las áreas de TI a los objetivos de las organizaciones".

"Considerar a la Seguridad Informática no como un conjunto de piezas tecnológicas, sino como una integración de procesos, personas y tecnologías".

"Apoyar al uso de tecnologías seguras, promoviendo productos y servicios de calidad".

"La cultura de las personas que toman decisiones en las empresas. Muchas de las personas en México no asocian la informática con riesgos, por lo que o no les preocupa la seguridad o prefieren no utilizar la tecnología para no tomar riesgos".

"Calidad de servicios informáticos. La gran mayoría de las empresas en México dependen de terceros para sus servicios informáticos: proveedores de enlaces, servicios de administración externos, etc. En muchos casos las empresas que proveen estos servicios no cuentan con el personal capacitado que entienda las implicaciones de las actividades que realizan.

"Disminuir la piratería. Una gran fuente de ataques en informática se deriva del uso de software pirata y de equipos no certificados.

"México no está aún preparado, en términos de leyes y regulaciones, para controlar el ya constante auge de delitos informáticos. Por lo que es necesario una reforma estructural en las leyes mexicanas".

Entre otros retos de importancia, se mencionaron:

"Implementar como estándar en las organizaciones el concepto de 'Information security officer'"

"Considerar la seguridad en las PyMEs como inversión y no un lujo".

"México requiere de más especialistas en esta área para poder cumplir con las necesidades en nuestro país. Perfeccionar a los que inician y desplazar a quienes dicen saber".

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

Se percibe una baja conciencia sobre riesgos, desconocimiento sobre temas de seguridad y un bajo nivel de desempeño de prácticas adecuadas dentro de las organizaciones. La mayoría de los expertos entrevistados mencionó que es indispensable promover una cultura laboral que tome a la Seguridad en Informática como parte fundamental del trabajo cotidiano, de los procesos y las políticas, en todos los niveles de la estructura organizacional de las empresas.

Es clara la necesidad de promover una mayor capacitación a nivel interno, que permita al personal de las empresas conocer más a fondo las posibles vulnerabilidades y cómo enfrentarse a ellas de una manera adecuada. De esta manera, tendrán la capacidad para actuar en la proporción necesaria.

Resalta también la opinión acerca de que no se está invirtiendo lo suficiente en tener y mantener infraestructuras informáticas seguras, principalmente en las pequeñas y medianas empresas.

Asimismo, se considera que deben reforzarse ciertas áreas y actividades dentro de las organizaciones, como son:

- Integración adecuada de todos los elementos que inciden y/o determinan la Seguridad en Informática.
- Recursos humanos competentes, en los puestos clave de las áreas de sistemas.
- Capacitación a los usuarios en general.
- Incorporación de modelos de arquitectura enfocadas a servicio.
- Eficiente gestión de accesos a información confidencial, así como esquemas de administración centralizada.

OBSERVACIONES MÁS **RELEVANTES**

"El principal reto de las empresas e instituciones usuarias es el ver a la seguridad informática como una parte integral de sus procesos diarios en donde la seguridad puede verse vulnerada, ya sea por un proceso no controlado, por personas que no estén del todo concientes del manejo de información o de lo que puede implicar una violación de seguridad informática.

"Institucionalización de procesos, políticas y procedimientos de Seguridad. Trabajar en la cultura laboral para hacer de la seguridad un punto clave de la operación diaria"

"Empresas Grandes: Integrar adecuadamente los diversos recursos de hardware, software, Consultoría (mejores prácticas) y Servicios para el desarrollo de proyectos que les permitan competir en mercados globales. Defenderse de los múltiples y constantes inténtenos de violación de sistemas por parte de usuarios externos o internos.
"PyMEs: Culturización de la importancia de la Seguridad Informática como un factor indispensable para la supervivencia de las empresas y acceso a procesos y tecnología masificada de bajo costo que les permita su adopción a este rango de empresas."

""Instaurar la posición de "Information Security Officer" (ISO) con la suficiente autoridad para implementar estándares y políticas de acceso a redes y PC's".

"Capacitación constante de recursos en temas de seguridad "estratégica" que les permita hacer inversiones, ya sea en modelos CAPEX o bien OPEX (según el modelo de ingresos de las mismas), de largo plazo".

"Incorporar modelos de Arquitecturas Orientadas a Servicio (SOA), en las que puedan centralizar la gestión y monitoreo de recursos, facilitar el cumplimiento de normas de la industria o gubernamentales y que les permita la reutilización de recursos tecnológicos para potenciar sus capacidades y reducir costos operativos".

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

Se percibe que es de suma importancia el rol que los fabricantes, distribuidores de equipo y software, consultores y desarrolladores de soluciones, juegan en la tarea de difundir, concienciar y capacitar a los usuarios en general y a las áreas competentes dentro de las instituciones. La mayoría de los expertos entrevistados mencionaron este papel de los proveedores como fundamental.

En cuanto a los productos propiamente, se considera que éstos deben ser liberados una vez que han sido probados perfectamente bajo estándares estrictos de seguridad. Además, los productos informáticos deberían salir al mercado con la seguridad integrada (no dejar la responsabilidad a desarrollos de terceros) y estar pre-configurados o ser fáciles de configurar.

El factor "precio" continúa siendo un elemento importante en la implementación de tecnología, de acuerdo a la opinión de un buen número de los entrevistados (23.5% de ellos hicieron alguna mención al respecto), entendiendo que no sólo se trata de bajar precios, sino de justificar un valor agregado tangible en el mismo.

Otros de los principales retos mencionados por los expertos, fueron los siguientes:

- Mantenerse actualizados, ofreciendo soluciones adecuadas para el entorno del país.
- Trabajar con las instituciones educativas para preparar personal calificado.
- Mayor oferta de soluciones de seguridad adecuadas para PyMEs.
- Conocer perfectamente las necesidades de sus clientes y su entorno.
- Ofrecer programas de actualización continua.
- Apoyar a las instituciones educativas con productos y material de laboratorio.
- Mayor flexibilidad para adaptarse a los mercados cambiantes.
- Disminuir o erradicar la práctica de la piratería.
- Financiamiento tecnológico.
- Mayor y mejor soporte tecnológico.
- Mejor Servicio a Clientes.

OBSERVACIONES MÁS **RELEVANTES**

"Tienen que hacer que sus productos sean probados y puestos en marcha en infraestructuras seguras".

"Incorporar la seguridad desde el inicio de la planeación de un software o del diseño de un hardware. Proveer de herramientas robustas no sólo en su funcionamiento, sino también en la seguridad".

"Deben conocer a fondo las preocupaciones y necesidades de sus potenciales Clientes, para poder ofrecerles las soluciones adecuadas y efectivas. También es importante estar actualizados con las problemáticas y riesgos que van surgiendo, como consecuencia de los avances tecnológicos y la globalización".

"Evangelizar a los usuarios en la importancia de la Seguridad Informática, haciéndolos concientes de que cuesta mucho más en todos aspectos la falta de seguridad que el uso adecuado de la misma".

"Hacer atractivos sus productos. Ofrecer paquetes a precios accesibles y con valor agregado (entrenamiento en línea, soporte técnico, etc.). Programas de actualización continua atractiva para el consumidor. Productos pre-configurados con perfiles específicos para facilitar la introducción de la tecnología a los usuarios. Apoyar a instituciones educativas proporcionando productos y material de laboratorio para que germine la cultura de Seguridad desde temprano en los usuarios".

"Financiamiento tecnológico, mayor y mejor soporte tecnológico, servicio a clientes".

"Venta de soluciones bajo un modelo de "venta consultiva" que les permita ofrecer proyectos de punta-a-punta y en los cuales se incorporen los elementos de seguridad que sean requeridos".

Entre otros retos de importancia, se mencionaron:

"Que puedan proveer sus productos con software de seguridad preinstalados".
"Constante escalabilidad y calidad de equipos y software.
"Establecer una estrategia de precios competitivos".
"Generación de servicios seguros "bajo demanda", que les permitan llegar a la mediana e incluso, a la pequeña empresa".

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

El apoyo para crear y fortalecer una cultura de seguridad en informática entre los habitantes de México, es sin duda la principal función que deberían ejercer las instituciones educativas, de acuerdo a las respuestas de los entrevistados. Una gran parte de ellos opina que estas instituciones deberían definir planes de estudio que toquen los tópicos más importantes de esta materia, desde edades tempranas y durante el transcurso de toda la educación (básica, media y superior). Se mencionó incluso, que a nivel universitario este tema debería formar parte de los programas de todas las carreras y no ser un tema exclusivo de aquéllas que están relacionadas con ingeniería.

Varios coincidieron en que estas instituciones, junto con el gobierno, son los principales entes que deberían promover y ejercer la mayor Investigación y Desarrollo en el renglón tecnológico. Si bien se está llevando a cabo actualmente, se considera que los esfuerzos son aún insuficientes.

Algunos consideraron que a la mayoría de las instituciones educativas todavía les falta mucho por hacer para mejorar su propia infraestructura de seguridad.

Otros retos y opiniones giraron alrededor de temas como los siguientes:

- Establecer alianzas estratégicas con los proveedores, para contar con productos y material de laboratorio.
- Preparar estudiantes en cantidad y calidad suficientes para satisfacer el mercado.
- Establecer alianzas con proveedores para mantenerse al día.
- Fungir como foros de opinión en la materia.
- Profundizar en el tema de ventajas y riesgos de seguridad en Internet.
- Ampliar programas de capacitación y especialización en Seguridad de la Información y de los panoramas legales que le rodean.
- Apoyo a empresas consumidoras de sistemas de seguridad y usuarios, en la difusión de temas relacionados. Creación de Consejos de Seguridad.

OBSERVACIONES MÁS **RELEVANTES**

"Dos temas: educar en las seguridad en informática e implantar sistemas de seguridad en las instituciones, que es donde hemos detectado un gran hueco".

"Ver a la Seguridad de la Información como una carrera de vida, la cual requiere de unas bases sólidas en todos los planes universitarios. El Internet y los riesgos que están rodeándolo, permiten enseñar la seguridad de la información no sólo a los ingenieros, sino a otras áreas, ya que harán uso de la misma tecnología".

"Preparar estudiantes en número suficiente y con la calidad y conocimientos necesarios para integrarse al mercado laboral, satisfaciendo la creciente necesidad de personal calificado. En conjunto con los Proveedores de hardware y software, establecer programas de actualización para cubrir los requerimientos de las instituciones (publicas y privadas)".

"Se requiere crear conciencia y base de conocimiento sobre temas de seguridad en TI desde etapas tempranas en la educación. Las instituciones educativas tienen una labor fuerte en cuanto a la definición de planes que cubran los tópicos más importantes en el área así como la orientación correcta a la audiencia, dependiendo del nivel de conocimiento, interés y necesidad.

JFS

Igualmente, se deben establecer relaciones estratégicas con empresas especializadas del ramo para cerrar los temas en conjunto y tratar de implementar escenarios de prácticas en laboratorios y recreación de casos reales. Esto mantiene en sincronía a estos dos mundos con el fin de tener una continuidad entre el ambiente estudiantil y el laboral (y favorecer el desarrollo de la cultura de seguridad)".

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

Más allá de la difusión y divulgación de temas relacionados, la cual se considera debería intensificarse, es importante que los propios medios de comunicación colaboren más de cerca con otros sectores, para crear conciencia entre la gente y fomentar una mayor cultura. La mejor manera en que lo podrían hacer, sería disminuyendo los tonos amarillistas y traduciendo los conceptos de riesgo y de soluciones, a un lenguaje que pueda ser entendido por el público al que van dirigidos (especializado para los expertos y sencillo y divertido para la sociedad en general).

Otros retos y opiniones mencionadas, trataron temas como los siguientes:

- Fortalecer su infraestructura de seguridad en informática
- Mayor capacitación a sus usuarios internos
- Diseminar campañas anti-piratería
- Homogeneizar conceptos y definiciones sobre este tema

OBSERVACIONES MÁS **RELEVANTES**

"La seguridad en informática tiene que se aprendida y divulgada por los medios de comunicación. Ellos pueden jugar un papel muy importante en la transmisión del conocimiento, así como en el compartir con los usuarios comunes y corrientes los problemas de seguridad y sus soluciones".

"Trabajar junto con las instituciones educativas, las empresas consultoras y los proveedores de hardware y software, para hacer consciencia entre los diferentes participantes del desarrollo del país, sobre la importancia de la adopción de la Seguridad Informática como una herramienta de competitividad indispensable para participar en la economía global. De no hacerlo, existe el riesgo de que el rezago del país se acentúe".

"Mayor difusión del problema para la población en general y desarrollar espacios específicos dentro de las secciones especializadas en tecnología dirigidas a pequeñas y medianas empresas".

"Hacer difusión de información que le permita al usuario no técnico entender los riesgos y como se puede defender".

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

Definitivamente, la acción que debería tomar el gobierno como su reto más importante, ha de estar encaminada a reforzar la legislación y regulación en la materia y garantizar su cumplimiento. Se percibe que no existen reglas claras para atacar los delitos cibernéticos y el enfrentamiento a la piratería es débil.

Asimismo, el gobierno y las asociaciones son agentes fundamentales en la difusión y fomento de la cultura en la materia, para promover y acelerar la adopción de medidas de Seguridad en Informática entre los diferentes sectores.

Dentro de sus funciones, debería estar también el establecer políticas y procedimientos en materia de seguridad de la información, así como el reforzamiento, con tecnología de seguridad, de la infraestructura a través de la cual brinda servicios al público.

Entre otras opiniones, también destacaron:

- Asignar presupuesto suficiente para la adquisición de herramientas de seguridad.
- Continuidad a los proyectos de largo plazo.
- Predicar con el ejemplo, teniendo su información protegida y segura.
- Mayor capacitación a sus usuarios internos.
- Promover la creación de fondos para apoyo a empresas en este rubro.
- Promover foros de opinión en la materia.
- Definir esquemas aceptables de identificación personal (firmas electrónicas)
- Apoyo a la capacitación en materia de Seguridad en Informática

OBSERVACIONES MÁS **RELEVANTES**

"El Gobierno y las asociaciones, juegan un rol crítico en la adopción de medidas de seguridad basadas en TI. Ante las empresas, organizaciones e instituciones, deberán ser promotoras de medidas de control interno y cumplimiento regulatorio que fortalezcan la operación de sus procesos, la calidad de sus servicios y que provean de certidumbre y credibilidad en las personas o entidades que interactúen con éstas".

"Reformas a las legislaciones actuales para tener un mejor marco legal, incorporar temas de privacidad de la información en forma electrónica, persecución de los delitos cibernéticos, aplicación de los mecanismos
necesarios para darle la integridad a las pruebas electrónicas, cadena de custodia y procedimientos del manejo de éstos.

"Continuidad y optimización de los proyectos de tecnología sin importar quien fue el promotor inicial o creador del mismo. Esto sucede con mucha frecuencia en nuestro país, ya que los cambios administrativos son consecuencia de renovación tecnológica".

"Desarrollo de un marco regulatorio que propicie el uso de los sistemas de Seguridad Informática, recompensando a las empresas e instituciones que la usen adecuadamente y apoyando mediante distintos medios (económicos y no económicos), a las empresas que vayan incorporando su uso productivo".

"El gobierno debe de ser un promotor de la seguridad y al mismo tiempo predicar con el ejemplo. Vemos que muchas instituciones gubernamentales manejan información muy confidencial, pero no cuentan con la
seguridad necesaria para asegurarla".

APORTACIONES RELACIONADAS CON SEGURIDAD EN INFORMÁTICA, HECHAS POR LAS EMPRESAS ENTREVISTADAS

3COM
Ignacio Leñero
Director General

"Damos Asesoría del estado de la seguridad en las empresas, implantamos sistemas de seguridad por medio de IPS, damos capacitación, servicio y contratos de mantenimiento y soporte".

ANDRESEN Y ASOCIADOS CONSULTORES
Carlos Carranza A.
Director General

"Concientizar a los Clientes de la necesidad de contar con políticas de seguridad Informática adecuadas y eficientes para sus empresas. Por un lado, no todos son bancos, ni tampoco misceláneas".

ASISTE
Moisés Polishuk
Director

"Respondemos a los problemas de robo de identidad y fraude electrónico".

BANORTE
Salvador Sierra Hernández
Director de Soporte Técnico e Infraestructura

"Uso de token para autenticación
Manejo de SSL en todos los sistema
Manejo de Certificados".

BOARD MEDIA
Dan Ostrosky Shejet
Consultor independiente

"En el caso de Seguridata (premio nacional de calidad 2005), desarrollando tecnología de Seguridad Informática de calidad y con reconocimiento a nivel mundial.

"Seguridata se ha convertido en un estándar de facto dentro del gobierno mexicano y esta participando en forma relevante en el desarrollo seguro de las cadenas productivas de diversas industrias".

CA SOFTWARE DE MÉXICO
Jorge Plascencia Zurita
Business Technologist

"CA está realizando múltiples aportaciones a la Seguridad Informática al considerarla como un foco en su visión de "Enterprise IT Management", dentro de las que destacan principalmente:

"Un liderazgo por varios años consecutivos de acuerdo a analistas independientes, los cuales colocan a CA como el proveedor #1 para soluciones de Administración de Identidad y Control de Acceso. Liderazgo que CA pretende mantener al continuar con el desarrollo de una solución que unifica y simplifica la administración de la seguridad a lo largo de toda la organización a través de la automatización y centralización de administración de políticas. Al integrar los mejores productos para proporcionar capacidades de Administración de Identidades y Control de Acceso completas, modulares y escalables. Así nuestras soluciones apoyan a las organizaciones a obtener desde identidades federadas hasta esquemas de autenticación fuerte, altas-bajas y cambios de identidades de usuarios y un soporte a esquemas de virtualización.

"Participación en los principales foros de definición de estándares y mejores prácticas como: Liberty Alliance, en lo referente a esquemas de Administración de Identidad y Control de Acceso para ambientes Web; ITIL al contar con el más grande número de consultores certificados en ITIL, y al mismo tiempo contar con personas que contribuyen directamente a la escritura y especificación de las mejores prácticas; entre otros foros.

"Así también CA está aportando a la Seguridad Informática una visión integral, modular y escalable, la cual contempla no únicamente soluciones tecnológicas, integra a profesionales certificados en las mejores prácticas y estándares de la industria, los cuales apoyan a las implantaciones de las soluciones enfocando cada implantación a cumplir con los controles y procesos de la organización; cabe mencionar que estos mismos profesionales, así como nuestros socios y aliados, son capaces de apoyar a las organizaciones en la formalización de sus procesos y controles. Otro factor que integra CA en su visión es el apoyar al personal de nuestros clientes con un área de capacitación la cual ofrece un variado catálogo de cursos que apoyan a este importante elemento a conocer y administrar de una mejor manera las soluciones tecnológicas que CA proporciona a sus clientes".

CABLEVISIÓN
Israel Madiedo Luna
Director de Sistemas de Red

"Al ser una empresa que brinda servicios de ISP, Video y Telecomunicaciones, debemos estar siempre a la vanguardia tecnológica en las áreas de TI y Comunicaciones. Esto no sólo es una práctica sino una filosofía de negocio.

"Constantemente se están actualizando las plataformas y sistemas de las redes de datos así como los sistemas que soportan las aplicaciones corporativas. Se cumple con estándares internacionales y se respaldan certificaciones de calidad y similares (como la Ley Sarbanes-Oxley).

"Buscamos aprovechar el talento de nuestros colaboradores internos y mantenerlos en un ambiente de libertad creativa y de investigación para poder desarrollar las mejores estrategias de Seguridad. Igualmente, tratamos de establecer relaciones de "socios tecnológicos" con nuestros proveedores para buscar, en conjunto, aquellos esquemas que nos permitan mantenernos al día y cumplir con el compromiso de brindar seguridad de TI a nuestros clientes internos y externos.

"La participación en foros, expos y conferencias nos ayuda a tener una visión actualizada de las tendencias de mayor influencia así como a participar en sesiones de retroalimentación con colegas del medio".

CITRIX SISTEMAS DE MÉXICO
Miranda Hernández Landavazo
Gerente de Mercadotecnia

"Las diferentes líneas de productos de Citrix se caracterizan por tener siempre un contenido de seguridad. Nuestro producto principal Citrix Presentation Server es en si un software seguro por diseño que permite a los usuarios acceder de forma segura a sus aplicaciones desde cualquier lugar, en cualquier momento y desde cualquier dispositivo".

INFOSINERGIA
Alejandro Romay Muñoz de Cote
Director General

"Participamos con CANIETI y AMITI en la elaboración de leyes en esta materia.

"Capacitamos a nuestro personal en estas tecnologías.

"Promovemos productos y servicios de calidad".

ITESM CAMPUS ESTADO DE MÉXICO
Francisco José Camargo Santacruz
Director de Informática

"Diplomado en seguridad informática.

"Especialización en seguridad informática en las carreras profesionales y en la maestría.

"Investigación en seguridad informática.

"Promoción de la cultura de seguridad en alumnos, empleados, padres de familia, egresados.

"Alianzas con empresas líderes en materia de seguridad informática (CA, Microsoft, IBM)".

JONIMA

Nils Olryd
Director General

"Ofrecemos productos para protección de información en los equipos con administración centralizada (encriptación, uso de perfiles, listas negras y blancas de software, etc.).

"Ofrecemos productos para asegurar la confiabilidad de la información (firmas electrónicas, factura electrónica, imágenes tridimensionales para cotejar información impresa fuera de línea, etc.).

"Servicios de administración de infraestructura con personal certificado y entrenado específicamente en las tecnologías que manejamos".

KIO NETWORKS

Diego F. Lastra S.
Chief Information Security Officer

1. *"Optimización de Infraestructura de Seguridad Informática.*

   "Hemos realizado importantes inversiones de infraestructura de Seguridad informática. Todas estas orientadas a productos de proveedores de servicios, que nos permite ofrecer servicios de alta calidad, con tiempos de puesta en operación muy bajos y sobre todo con una relación precio beneficio bastante atractivo en el mercado mexicano. De esta manera aportamos significativamente a la rápida gestación de nuevas empresas y ayudamos a las grandes a ir más rápido en la carrera tecnológica.

2) *"Nuestro principal interés esta relacionado con satisfacer las necesidades del cliente y siempre ir un paso más allá. Nuestro negocio no está ligado a productos en específico, lo cual nos da un excelente margen de maniobra para satisfacer al máximo las necesidades de nuestros clientes, Confidencialidad, Integridad y Disponibilidad. Todas nuestras soluciones son "un traje a la medida" lo cual ayuda a crecer más rápido a las empresas, olvidarse del factor tecnológico y dedicarse exclusivamente a los factores de éxito y del mercado.*

3) *"Estamos totalmente comprometidos con la seguridad informática y su vital importancia en todos los ámbitos. Por tal motivo ofrecemos a nuestros futuros clientes cursos de "Security Awareness" (Concienciación de Seguridad Informática) sin costo alguno, el cual nos ayuda mutuamente a fortalecer una cultura de seguridad informática en México".*

MATTICA

Andrés Velásquez
Director de Investigaciones Digitales

"Mattica es hoy en día, el primer laboratorio e-forense de México, donde se realizan diariamente acciones de capacitación, asesoría y seguimiento de los delitos informáticos no sólo a la iniciativa privada, sino también a las agencias gubernamentales que lo soliciten en todo Latinoamérica".

MEXIS, SEGURIDAD ADMINISTRADA

Antonio Llausás Zamarripa
Director Comercial y de Alianzas

Jorge J. Díaz Denis
Director de Desarrollo de Productos y Mercadotecnia

"Hoy en día Mexis, implementa, monitorea y administra la seguridad de más de 200 compañías en México, ha realizado grandes inversiones en cuestión tecnológica para poder mantener los niveles y estándares de respuesta con el objetivo de contrarrestar los riesgos informáticos. Por otra parte, Mexis realiza seminarios y eventos que permitan dar a conocer día a día las nuevas tendencias sobre vulnerabilidades informáticas".

QOS LABS DE MÉXICO

Iván Santacruz Ortiz
Director de Mercadotecnia

"QoS Labs se ha especializado en el desarrollo e implementación de soluciones basadas en Gestión de Identidad, Acceso y Aprovisionamiento; pudiendo auxiliar a las empresas que buscan fortalecer su estrategia de seguridad e integrarla a una arquitectura de componentes re-utilizables y altamente escalables".

SIEMENS

Arturo Olguin Alpizar
Subdirector OI

"A nivel mundial se han establecido y publicado medidas y políticas de seguridad muy estrictas, que nos han permitido bajar los riesgos de ataques e infecciones a nuestra red.

"Fue nominado un ISO por país y un ISA (Information Security Advisor) por departamento, los cuales tienen la responsabilidad de difundir, implementar y vigilar que se apliquen todas nuestras políticas de seguridad.

"Se hace un escaneo periódico (por mes) de vulnerabilidades de cualquier dispositivo conectado a nuestra red, del cual los resultados son publicados a nivel regional (p.e. LATAM, Asía, etc.)".

IV. CONCLUSIONES DE LA INVESTIGACIÓN

PANORAMA GENERAL

México ha sido catalogado por los expertos como un país aún inmaduro en materia de Seguridad en Informática. Desde luego, se han registrado avances importantes en los últimos 3 años, al subir los niveles de conciencia y conocimiento de los usuarios acerca de los principales riesgos a los que podrían estar expuestos, sobre todo hablando del ámbito de Internet. Sin embargo esta conciencia no se refleja aún en prácticas a nivel personal ni empresarial. Hace falta una mayor difusión en este rubro, percibido tanto por los expertos como por los usuarios encuestados.

JFS

En el ámbito de los corporativos y grandes organizaciones, privadas y gubernamentales, los niveles de conciencia e implementación, suelen estar en un nivel equiparable a la de los países más desarrollados. El ejemplo de la banca mexicana fue muy mencionado por todos los grupos de entrevistados, sector que, por lo que corresponde al manejo de dinero de manera electrónica, ha tenido que ponerse a la vanguardia.

Si bien, como en los estudios anteriores, los virus fueron percibidos como la principal amenaza para los equipos de cómputo y su información, bajó significativamente la frecuencia de menciones como concepto aislado. Los usuarios tienden a hablar cada vez más de la inseguridad como un problema integral de varios elementos e identifican una mayor importancia hacia aspectos como la privacidad y confidencialidad, la transmisión segura de datos, el robo de identidad, etc.

Llama poderosamente la atención que el 13.5% de todos los entrevistados mencionaron las políticas y procedimientos adecuados como uno de los aspectos primordiales y, entre usuarios que trabajan en áreas de informática, el 33.5% están conscientes de la importancia de este rubro. Esto muestra un importante avance, respecto de los estudios anteriores, y permite ver que el nivel de conciencia está mejorando en el país. Sin embargo,, únicamente el 6.3% mencionó que le gustaría saber más acerca de políticas y procedimientos, así como mejores prácticas a nivel mundial.

Entre los usuarios comunes, destacan dos preocupaciones expresadas con mucho mayor frecuencia que en años anteriores. Una es la confidencialidad de la información almacenada en los equipos de cómputo de sus empresas, principalmente la relacionada con su correo electrónico, seguida de sus documentos. Existe un claro temor a que terceros intervengan sus correos o puedan acceder a sus equipos sin autorización. La otra gira alrededor de las compras en línea y la utilización de la banca electrónica. Los usuarios están cada vez más conscientes del hecho de que la seguridad en informática está ligada a elementos personales, y que el comprometer los datos privados, tanto de una empresa como de una persona, es un riesgo sumamente importante.

Si bien se perciben avances en la cultura sobre seguridad informática en general, se nota claramente una falta de difusión en este sentido, principalmente en algunas áreas que presentan huecos importantes. La preocupación en aspectos como virus, spyware y firewalls, muestra que los usuarios siguen considerando que gran parte del problema se resuelve con soluciones tecnológicas, haciendo a un lado la responsabilidad personal que tiene cada usuario de llevar a cabo las prácticas adecuadas. Esta difusión y adquisición de conocimiento no sólo debe recaer en los proveedores de tecnología, sino en las áreas responsables de informática y, de manera importante, en cada usuario.

COINCIDENCIAS Y DIFERENCIAS ENTRE EL USUARIO "INFORMÁTICO" Y EL "NO INFORMÁTICO"

Es previsible, dadas las diferentes actividades y preparación, que existan ciertas diferencias de opinión entre los usuarios Informáticos (grupo compuesto por ejecutivos que se encuentran a cargo de un área de sistemas o que, en el caso de empresas pequeñas, tienen bajo su responsabilidad las cuestiones relacionadas con informática) y los No Informáticos (grupo compuesto por ejecutivos de otras áreas, como administración, producción, ventas, mercadotecnia, operaciones, legal, etc.). En efecto, fueron más las diferencias encontradas que las coincidencias entre ambos grupos, aunque es claro que en algunos aspectos, comparten demandas similares.

Coincidencias

- De manera consistente con los estudios de 2004 y 2005, para ambos grupos los virus son considerados como una de las amenazas más importantes (la primera para los No Informáticos y la segunda para los Informáticos). No es de extrañar, que una de las principales medidas sugeridas por ellos para proteger la información y los equipos de cómputo, sea precisamente el Antivirus.
- Entienden a la transmisión segura de datos como uno de los aspectos principales que componen la Seguridad en Informática.
- Ambos grupos colocan a la confidencialidad de la información en un nivel similar de importancia.
- Las tres principales medidas de ambos grupos para tener redes inalámbricas seguras, fueron:
  - Controles de acceso y autenticación (tanto para acceso físico a las instalaciones, como para acceder a los equipos y a la información).
  - Herramientas de protección local (a nivel servidores o PCs), como antivirus, antispyware, antispam y firewalls.
  - Encripción de datos.
- En cuanto a los diversos elementos que son indispensables para comprobar la identidad de un usuario de manera electrónica, ambos grupos mencionaron, como los principales, el uso de la combinación Nombre de Usuario y Contraseña, seguida de los dispositivos biométricos. Es importante ver que el usuario en general se está volviendo más sofisticado y conocedor. El 27.6% (más de la cuarta parte) de los entrevistados totales mencionaron en algún momento los elementos biométricos como soluciones de seguridad.
- Los 5 temas principales sobre los cuales los miembros de ambos grupos quisieran profundizar, en el mismo orden, fueron los siguientes:
  - Seguridad en Informática en general.
  - Avances, tendencias y actualizaciones.
  - Costo-Beneficio de los diferentes productos y servicios ofertados.
  - Políticas y procedimientos, así como mejores prácticas a nivel mundial.
  - Normatividad y regulación.

Diferencias

Usuarios informáticos

- Aparte de la transmisión segura de datos, en donde hubo coincidencia en ambos grupos, los principales conceptos alrededor de la Seguridad en Informática para este grupo fueron el Acceso Controlado, así como la Integridad y Confiabilidad de la Información.
- La mayor preocupación sobre el tema para este grupo, fue la Integridad de la Información, seguida por los Virus, la Confidencialidad y los ataques de spyware y adware.
- Este grupo mostró mayor conocimiento y preferencia por soluciones como los firewalls, proxys, respaldos de información, creación de políticas y procedimientos, como medidas para reforzar la seguridad de sus equipos y aplicaciones.
- Una mayor proporción de Informáticos, frente a los No Informáticos, está consciente de los beneficios de los certificados y firmas electrónicas como elementos de comprobación de identidad, así como de los dispositivos de clave dinámica (token o confirmaciones vía SMS/e-mail).

Usuarios "No Informáticos"

- Los principales conceptos alrededor de la Seguridad en Informática para este grupo,

fueron la Privacidad y Confidencialidad de la información, así como la Protección Contra Virus.

- Para los No Informáticos la seguridad ante el robo de identidad, resulta fundamental. En el estudio anterior, ningún miembro de este grupo lo mencionó como la amenaza de mayor riesgo, mientras que en 2007 fue mencionado por el 6.5% de los No Informáticos entrevistados. También se percibe un mayor conocimiento, entre este grupo, sobre el software espía y sus consecuencias,
- Este grupo dio mucho mayor peso a preocupaciones como la Pérdida de Información, la Invasión a la Privacidad y a las Compras en Línea, que los Informáticos.
- Las "preguntas clave" o preguntas secretas, están más presentes en este grupo de entrevistados, como una solución para identificar al usuario electrónicamente.

PRINCIPALES DEMANDAS POR PARTE DE LOS USUARIOS

Se percibe una mayor conciencia y conocimiento acerca de soluciones contra intrusos, spyware, spam, etc. Los usuarios de ambos grupos demandan, de manera más enfática, que se hagan mejoras constantes en estos rubros.

Coinciden tanto informáticos como No informáticos en que hace falta una mayor difusión por parte de los proveedores de tecnología, encaminada a crear una mayor cultura sobre seguridad en informática. Es importante recalcar que ambos grupos solicitan que esta información sea fácil de entender de tal manera que personas no especializadas tengan elementos para seguir prácticas seguras en el desempeño de su trabajo. La mayoría de los expertos entrevistados mencionaron este papel de los proveedores como fundamental, además de una buena oferta de productos y servicios.

PRINCIPALES RETOS PARA LAS ENTIDADES ORGANIZADAS DE MÉXICO

La inversión en protección de infraestructura e información, de manera general, resulta insuficiente, principalmente en las empresas medianas y pequeñas. Aunque una de las demandas del personal de TI de las empresas giró en torno a precios más competitivos, no se percibe que ésta sea la causa principal de los rezagos en esta materia. Es más una cuestión de comunicación, educación, políticas, procedimientos y definición y/o adopción de estándares.

Un renglón en donde se percibe un rezago significativo, es en el área de normatividad y regulación. Se percibe que no existen leyes claras, que permitan sancionar adecuadamente e intimidar a los delincuentes informáticos. Tampoco se percibe voluntad de las autoridades por atacar a la piratería, la cual es considerada como una fuente de riesgos, ya que los usuarios instalan aplicaciones de origen desconocido, supuestamente productos de marca, que en la mayoría de los casos no pueden ser actualizados con los parches, versiones y definiciones, que constantemente se producen precisamente para dar mayor seguridad a los programas. Asimismo, haciendo un análisis comparativo con los resultados de los dos estudios anteriores, se percibe que un porcentaje significativo de los entrevistados (5.7% de la muestra total), mostró interés por temas relacionados con la normatividad y legislación en la materia, contra una frecuencia menor al 0.7% en el estudio de 2005.

V. ARTÍCULOS SOBRE SEGURIDAD EN INFORMÁTICA

Análisis y evaluación de riesgos en TI

Por Adrián Palma
Presidente de la Asociación Latinoamericana de Profesionales
en Seguridad Informática (ALAPSI)

Mi primera participación en un proceso de Análisis y Evaluación de Riesgos (AER) en la vida real fue en el año de 1996, cuando trabajaba para una firma internacional. Aunque ya contaba con cierto conocimiento teórico en la materia, en ese momento entendí 2 cosas que marcarían mi vida profesional: la primera es que el AER es el factor crítico de éxito para cualquier proyecto relacionado con la seguridad en Tecnologías de Información (TI) y la segunda es que este tipo de proyectos son muy difíciles de entender, vender y justificar a la alta dirección, ya que hablar de riesgos en tecnología es complejo, los resultados son de alguna manera intangibles y el retorno de la inversión es complicado de demostrar, pero una vez que éstos son entendidos, créanmelo, los resultados son de mucha valía para cualquier organización teniendo en cuenta que el AER se ejecutó de forma correcta. El tema me apasionó y me propuse conocer más a fondo de todo lo relacionado con los riesgos en TI, desde sus inicios, enfoques (cuantitativos y cualitativos), metodologías, modelos, herramientas etc. etc.

El AER inicialmente tuvo un enfoque cuantitativo, ya que en ese tiempo los ambientes de procesamiento eran totalmente centralizados y era mucho más sencillo cuantificar el valor de los activos y la probabilidad de ocurrencia de las amenazas para así poder calcular, por fórmulas matemáticas, la pérdida en dinero y del impacto de la materialización de un riesgo. Este tipo de enfoque hoy día, desde mi punto de vista, es obsoleto e impráctico, ya que la dificultad de poder obtener datos precisos de probabilidades de ocurrencia de las amenazas, es muy difícil.

Con el paso del tiempo el AER cambió a un enfoque cualitativo, que es el más usado hoy día y que presenta los riesgos de una organización clasificados en altos, medios y bajos. En mi experiencia, las organizaciones no requieren saber el 3.1416, es decir, la precisión de los valores del riesgo, sino cuáles son aquellos riesgos que pudieran poner en peligro la capacidad de operación, el servicio o, en algunos casos, la supervivencia de la organización y contestar la pregunta mas importante ¿qué nivel de seguridad requiere mi organización?.

La alta dirección de cualquier organización tiene la responsabilidad de poner atención, atender y facilitar lo necesario para llevar a cabo un AER en su organización (llamado en inglés el "Due Diligence"). Este concepto en otros países está legislado; hoy día en nuestro país, en algunos sectores (Financiero, Empresas Trasnacionales), empieza a ser una cuestión de "compliance" (cumplimiento) dentro de estas organizaciones, pero debemos entender que si este tipo de proyectos no es apoyado por la alta dirección, será prácticamente imposible que se lleve a cabo.

La causa principal por la que fallan los AER es porque su alcance está limitado a las áreas de TI y no a las áreas de negocio o funcionales. Recordemos que la función de TI es totalmente de servicio para dichas áreas, por lo que cuando se trate de mitigar los riesgos tecnológicos, éstos deben ser los que afecten a las áreas funcionales o de negocio de la organización. Un AER debe completarse en semanas, no en meses o años, y debe ser eficaz, eficiente y asertivo, para que tenga el impacto esperado.

Para ser efectivo, el proceso de análisis y evaluación de riesgos debe ser aceptado como parte del proceso del negocio de la empresa. El profesional de seguridad en Tecnologías de Información (TI) busca asegurar que el

proceso de análisis y evaluación apoyen los objetivos del negocio o la misión de la organización. Hay que recordar que parte del éxito de un proceso de análisis y evaluación de riesgos, es su aceptación por parte de todo el personal de la organización. Tratar de imponer la seguridad a la alta dirección sin fundamentos puede resultar contraproducente. Un proceso de análisis y evaluación de riesgos efectivo buscará las necesidades reales de la organización e involucrara a los dueños de la información

La mayoría de los enfoques del proceso de análisis de riesgo se basan en el triángulo CID que contiene los 3 principios de seguridad de la información: Integridad, Confidencialidad y Disponibilidad.

JFS

Cada organización tiene que establecer su propio conjunto de requisitos para la protección de sus activos de información (datos, hardware, software, redes, sistemas operativos, bases de datos, aplicaciones, instalaciones, personal, dinero, procesos de negocio etc.). Esto es comúnmente documentado a través de una política de clasificación de la información. Los controles diferirán dependiendo de la sensitividad y criticidad del activo de información. Por lo tanto, la meta de un programa de seguridad de la información a lo largo de una empresa y de un proceso de análisis y evaluación de riesgos, es determinar el impacto de la materialización de las amenazas en los activos de información, basado en:

- **Integridad:** Se requiere que la información no sea modificada inapropiadamente.
- **Confidencialidad:** La información es protegida del acceso no autorizado o la divulgación accidental.
- **Disponibilidad:** los usuarios autorizados pueden acceder a la información cuando lo requieran para realizar su trabajo.

El proceso de clasificar la información necesita estar perfectamente definido, y se requiere implementar una metodología para ayudar a los usuarios a determinar el nivel de clasificación como parte del proceso de análisis y evaluación de riesgos.

Estos pueden incluir algunos, todos, o más de los siguientes:

- El costo de producir la información.
- El valor de la información en el mercado.
- El costo de reproducir la información si fuera destruida.
- El beneficio que trae la información a la empresa al cumplir los objetivos del negocio o de la misión.
- Las repercusiones para la empresa si la información no está disponible.
- La ventaja que se le daría a la competencia si pudiera usar, cambiar o destruir la información.
- El costo para la empresa si la información fuera divulgada, alterada o destruida.
- La pérdida de confianza del cliente o la pérdida del cliente si la información no es segura.
- La pérdida de imagen y pérdida de negocio, además de sanciones, por no tener información segura.

El valor del activo de información debe ser determinado por el dueño de la misma, donde la información es creada o es el usuario principal de ese recurso.

LA METODOLOGÍA DEL ANÁLISIS Y EVALUACIÓN DE RIESGOS

El proceso de análisis y evaluación de riesgos comúnmente consta de cinco elementos: los activos de información, las amenazas identificadas, las vulnerabilidades identificadas, el nivel de riesgo establecido y los controles seleccionados.

ACTIVOS DE INFORMACIÓN

Un financiero podría decir que un activo es algo que tiene un valor. Sin embargo, los activos de información físicos o tangibles no son los únicos activos que deben protegerse; también tenemos que proteger aquellos activos intangibles, como la imagen, la propiedad intelectual, etc.

IDENTIFICACIÓN DE LA AMENAZA

Después de que se ha identificado el activo que necesita ser protegido, se deben identificar las amenazas que podrían afectar a los activos involucrados en el análisis y evaluación de riesgos.

Existen tres fuentes comunes para las amenazas y pueden ser clasificadas como naturales, humanas o ambientales. Recuerde que la categoría humana esta dividida en dos subcategorías: accidentales y deliberadas. Tal y como hemos mencionado antes, las amenazas humanas deben ser vistas a través de actos deliberados como los ataques por personas maliciosas o empleados a disgusto, o de actos sin intención, como la negligencia o los errores.

ELEMENTOS DE AMENAZA.

Al examinar las amenazas, los expertos identifican tres elementos que están asociados con la amenaza.

- El agente catalizador que realiza la amenaza. El agente puede ser humano, una máquina o la naturaleza.
- El motivo es algo que causa que un agente actúe. Estas acciones pueden ser accidentales o deliberadas.
- Los resultados son la amenaza materializada. Durante el proceso de evaluación de riesgo será necesario identificar tantas amenazas como sea posible. Identificar una amenaza es sólo la primera parte de la fase del análisis. Será necesario determinar qué tan vulnerable es su empresa a esa amenaza.

DETERMINACIÓN DEL NIVEL DE RIESGO

Al examinar la amenaza, existen dos formas claves de evaluar la probabilidad e impacto. El primer método es establecer la probabilidad sin la consideración de los controles existentes. El otro método es examinar el nivel de riesgo tomando en cuenta los controles existentes. Esto permitirá al equipo examinar los controles existentes y establecer un nivel de riesgo basado en qué tan eficaces son. La probabilidad a la que es susceptible una organización respecto a una amenaza específica, se describe típicamente como alta, media o baja.

El siguiente paso es preguntarse ¿qué se va a hacer con los riesgos? Esta etapa es conocida como el manejo o la administración del riesgo (Risk Management) y básicamente hay 3 alternativas; una es **tolerar** el riesgo (no se implementan controles), otra es **transferir el** riesgo (se transfiere el riesgo a un tercero) y la última es **mitigar** el riesgo (se implementan controles). Esta alternativa es la que tiene un peso mayor en el proceso del AER, ya que en ésta se buscará que la organización tenga un nivel aceptable de riesgos. Por consiguiente, será importante identificar tantos controles como sea posible. En esta etapa se requiere la participación de especialistas de seguridad.

Al seleccionar cualquier tipo de control será necesario medir el impacto operacional para la organización. Cada control tendrá un impacto de alguna manera.

El costo de los controles debe ser analizado y evaluado detalladamente. Una buena regla de dedo es evaluar, si el control es más caro que el activo que va a proteger, no se debe implementar. Durante esta etapa se podrá determinar si se requieren controles de seguridad basados en algún estándar, como El Código de Prácticas para la Gestión de la Seguridad de la Información (ISO/IEC 17799-1, BS7799-2 hasta Diciembre del 2005 o el ISO27001 a partir del 2006), La ley Gramm Leach Bliley (GLBA) o la ley Sarbanes Oxley (SOX).

ANÁLISIS COSTO-BENEFICIO

Después de identificar todos los controles posibles y evaluar su viabilidad y efectividad, se debe realizar un análisis costo-beneficio. Este proceso debe ser realizado para cada control, a fin de determinar si el control recomendado es apropiado para la organización.

Al realizar un análisis de costo-beneficio es necesario considerar el costo de implementación basado en los siguientes factores:

- Costo de implementación, incluyendo la inversión inicial para el software y hardware, como mantenimientos, soporte etc.
- Reducción de efectividad operacional.
- Implementación de políticas adicionales y procedimientos para apoyar a los controles.
- El costo de la capacitación que apoye al personal a mantener la efectividad del control.

CONCLUSIONES

Prácticamente ningún activo o actividad está libre de riesgo y no todos los controles implementados pueden eliminar el riesgo. El propósito de manejar los riesgos es tener a la organización con el nivel de seguridad que realmente requiere, para tener un nivel aceptable de riesgo, que la operación y la capacidad de servicio no se vean afectadas por la implementación de controles, además de que la inversión sea razonable, es decir, que no se hagan erogaciones cuantiosas e innecesarias. Un programa de seguridad que tiene como meta el 100% de seguridad, causará que la organización tenga 0% de productividad, teniendo en cuenta que ningún control mitigará el 100% del riesgo, siempre habrá un remanente llamado Riesgo Residual.

Seguridad alineada al negocio

Por Jorge Plascencia Zurita
Business Technologist
CA Software de México

JFS

En los últimos meses hemos notado, tanto los profesionales de TI y de la Seguridad Informática, como todos los usuarios de sistemas electrónicos, una creciente necesidad de incrementar nuestra seguridad, ya no en las áreas perimetrales de nuestras empresas y computadoras, ahora tenemos la necesidad de proteger nuestra privacidad, confidencialidad e identidades, pero al mismo tiempo no podemos aislarnos del mundo. Es decir, requerimos de mantener nuestra o nuestras identidades electrónicas privadas, pero al mismo tiempo tenemos que compartirlas con varias entidades, como nuestros proveedores de tarjetas de crédito, banca electrónica, correo electrónico, etc.

Lo anterior está llevando a la seguridad informática a un nuevo territorio, en el que ya no se trata de construir barreras alrededor de la información, ahora tenemos que, sí, mantener nuestras barreras, pero al mismo tiempo crear túneles y canales con nuestros socios, amigos, proveedores y personas que nos interesa tengan acceso a parte de nuestra información. Si a esto aunamos la necesidad de las organizaciones y personas de invertir adecuadamente los recursos, vemos que nuestras barreras y túneles deben de estar completamente alienados a los objetivos de nuestra organización, empresa o planeación personal.

Por lo anterior, en CA nos hemos preocupado de brindar una solución de seguridad completamente modular e integrada, la cual, complementada con la experiencia de consultores de varios niveles, puede ser perfectamente alineada a sus objetivos. Lo anterior lo hemos logrado integrando a una visión de Unificación y Simplificación, tanto de usuarios como de activos, lo que nos permite apoyar los servicios que las áreas de TI entregan para apoyar y soportar a los procesos de negocio de las organizaciones.

Para lograr este objetivo hemos integrado una solución de seguridad integral la cual se enfoca en la Administración de Seguridad, desde las amenazas tradicionales como virus y spyware, hasta la Administración de Identidades, Control de Acceso e Integración, filtrado y correlación de eventos de seguridad, así como también Análisis Forense. Lo anterior se integró con la finalidad de ayudar a las organizaciones a responder preguntas cruciales como: ¿Qué está pasando en mi ambiente? ¿Qué puedo y debo hacer al respecto? ¿Quién tiene acceso a qué? ¿Qué ha hecho en el sistema?

Así pues, CA se enfoca en soluciones que le permiten llevar a cabo una visión de seguridad alineada con los objetivos de su empresa u organización, no únicamente apoyada en tecnología, sino apoyada en las mejores prácticas y consultores especializados que le permitirán ver Retornos de Inversión y Administración de Riesgos.

La Seguridad Informática en las escuelas

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

Es difícil entender la primera década del Siglo XXI, sin la transformación que ha significado en el mundo la participación de la tecnología aplicada en favor de la educación.

Los expertos afirman que las Tecnologías de la Información y Comunicaciones (TIC), serán una herramienta tan común en el proceso educativo a finales de esta década, como los lápices o las gomas de borrar.

No cabe duda de que en la actualidad las escuelas están más conectadas que nunca y que muchos estudiantes han adelantado a profesores y a padres, para convertirse en expertos en Internet.

La seguridad informática entonces se ha convertido en un elemento fundamental en el proceso educativo que, al igual que en cualquier proceso, debe contemplar con el mismo énfasis las amenazas externas y las internas, diferenciando la casuística del ámbito en la que estos riesgos se enmarcan.

Un informe publicado en el último año por el Centro Nacional de Estadísticas en Educación de los Estados Unidos, (National Center for Education Statistics) determinó que el 99 % de las escuelas públicas K-12 de los Estados Unidos estaban conectadas a Internet, y que el 94 % de las computadoras dispone de conexión de banda ancha de alta velocidad.

De la misma forma en México es cada día mayor el número de aulas con computadoras conectadas a Internet, lo cual ha hecho crecer la importancia de entender y aplicar correctamente los procesos de seguridad informática en todos sus contextos.

La introducción de la tecnología de Internet en las aulas ofrece muchos beneficios que pueden perderse si los usuarios no están bien informados o si la tecnología no está correctamente protegida.

Para conseguir protegerse de las amenazas potenciales, es inevitable la definición y puesta en marcha de un plan de seguridad que evalúe la realidad del sistema, detecte las necesidades y aplique las medidas protectoras adecuadas al nivel de seguridad buscado.

No se trata de aplicar seguridad por aplicarla. Se trata de hacerla coherente y posible. Un plan de seguridad debe ocuparse de definir medidas que protejan los recursos frente a cualquier amenaza, tanto externa como interna, identificando claramente qué se protege, por qué y cómo.

En términos generales, **la seguridad de la tecnología en las escuelas debe tratarse con un enfoque empresarial.** Del mismo modo que todas las empresas poseen datos financieros e información de clientes confidenciales, las redes de escuelas también guardan información confidencial, incluyendo registros detallados de estudiantes con sus direcciones y números de la cédula de identidad, además de las notas, que son frecuentemente un blanco tentador para los alumnos.

Debe recoger procedimientos de protección y medidas correctoras de respuesta en caso que se produzca algún incidente. Una actitud de gestión, más que una aptitud, que no sólo debe ser entendida como una buena práctica de administración. No hay que olvidar que la elaboración e implantación de un plan de seguridad puede ser exigible, incluso, desde el punto de vista legal, pudiendo acarrear consecuencias jurídicas su ausencia, tanto si se producen percances de seguridad como si no ocurren.

De cara a elaborar un buen plan de seguridad en un proceso de educación, en cualquiera de sus niveles, suele

ser lo más conveniente recurrir a terceros, a empresas especializadas en este tipo de análisis, que de forma objetiva e independiente, tienen mejor capacidad para identificar los riesgos, las vulnerabilidades presentes y las medidas correctoras que interesa aplicar.

Al exteriorizar la elaboración del plan se seguridad, al contratar una auditoría externa, se evita desviar recursos humanos y técnicos propios que siempre resultan escasos, críticos para mantener el sistema en funcionamiento. El coste que supone una auditoría de estas características, queda de sobra compensado con la reducción de tiempo en el análisis y despliegue de la estrategia de protección. El tiempo que se tarda en elaborar y aplicar el plan de seguridad, es el tiempo durante el cual la posibilidad de materialización de cualquier amenaza es mayor.

JFS

Las redes de las escuelas necesitan, además, protección contra amenazas, tanto internas como externas. En muchos casos, la violación de la seguridad es consecuencia de la falta de conocimiento o entrenamiento de los usuarios en prácticas informáticas seguras. En otros casos, el problema reside en estudiantes que intentan invadir los servidores y computadoras de la escuela.

En cualquier caso, para conseguir implantar un buen plan de seguridad es imprescindible crear una "cultura de seguridad" entre los usuarios, que les haga partícipes y les implique en su efectiva aplicación.

Dar publicidad sobre normas de obligado cumplimiento, recomendaciones sobre cómo llevar a cabo determinadas operaciones, consejos y todo tipo de información relacionada, puede evitar que técnicas como la ingeniería social no tengan predicamento entre el personal de la escuela, puede revelar posibles brechas de seguridad inadvertidas o, sencillamente, alertar sobre comportamientos y actitudes que puedan dar lugar a incidentes si no se previenen a tiempo.

La lucha contra virus y SPAM puede ser el ejemplo más cotidiano e inmediato de este interés. Unos usuarios concienciados y bien aleccionados suponen el primer filtro más eficaz para impedir la propagación de código malicioso de todo tipo en la red propia.

El uso generalizado de computadoras conectadas a Internet exige que los administradores de la escuela, bibliotecarios, profesores, estudiantes y sus familiares, se aseguren de utilizar los equipos de manera apropiada y segura. Los programas de seguridad informática eficaces incluyen la concienciación y apoyo de los usuarios para que se reduzcan los riesgos. La definición de políticas y procedimientos preparan el escenario de la informática segura. Es necesario educar a los usuarios, ya que, de lo contrario, podrían convertirse involuntariamente en el origen de las brechas en la seguridad.

Las computadoras preparadas para el uso de Internet en clase pueden ofrecer una gran contribución a las principales metas de enseñanza y aprendizaje de la escuela, siempre y cuando se adopten pasos proactivos para proteger la tecnología y educar a los usuarios.

¿Qué tan segura es tu red y tus servicios hoy día?

Por Adrián Rodríguez
Solution Specialist
Intel México

Un tema que cobra más importancia en esto días es la seguridad. Ya no sólo se habla de seguridad en las calles sino que ahora tenemos que hablar de la seguridad en la carretera de la información que es Internet. Los ataques en este sentido van en aumento; tan es así, que ahora se está sugiriendo tipificar los crímenes ahí cometidos, ya que éstos están llegando a cifras millonarias en muchos sentidos, desde los que sufren algún tipo de fraude electrónico hasta las empresas que son atacadas todos los días con los virus informáticos que ocasionan pérdidas millonarias a las mismas.

¿Cuánto cuesta hoy día un ataque de un virus en una empresa? ¿Cuál es el costo de tener un servicio informático fuera de línea? ¿Cuánto cuesta tener a un usuario fuera de línea? No estamos muy lejos en pensar y saber que un virus puede ser la diferencia entre cerrar un negocio o no, ofrecer un servicio e incluso, en el peor de los casos, perder información valiosa y millonaria, la cual es crucial para la existencia de las empresas.

Seguridad y conveniencia son dos cosas que típicamente son vistas como objetos de conflicto, sin embargo esto no tiene por qué seguir siendo así, ya que hoy día podemos tenerlas ambas para crear una infraestructura de TI segura.

En la actualidad las redes informáticas enfrentan muchos riesgos de seguridad sin importar si son redes alámbricas o inalámbricas. Uno de los más comunes es el acceso no autorizado. Además de éstos, debemos protegernos de los daños al interior de la empresa que son las más comunes, muchas veces por conocimiento y algunas otras por desconocimiento.

¿Pero cómo hacemos para negar el acceso a la red, a los dispositivos contaminados, sospechosos o que no cumplen con todas las normas de seguridad, obviamente sin perder la productividad? Cuando se detecta que un equipo conectado a la red no cumple con los requerimientos mínimos de seguridad, desconectarlo de la misma no es suficiente. Los gusanos informáticos (worms), por ejemplo, se propagan de manera automática rápidamente a través de la red. Para mejorar la protección, un equipo contaminado no debe de ser admitido en la red nuevamente si no ha sido corregido el problema.

Las redes alámbricas tienen la ventaja de requerir un acceso físico para conectarse a la red. Como resultado de esto, nos permite contar con una protección parcial, como personal de seguridad y puertas cerradas para no permitir los accesos. Sin embargo, aún con la seguridad física, las redes alámbricas presentan los mismos riesgos de virus y gusanos que las redes inalámbricas, además de que se debe proteger de los usuarios autorizados dentro de la red que se quieran conectar a lugares o información no autorizada.

Por su naturaleza, las redes inalámbricas no requieren de dispositivos físicos para su conexión, aunque por esto no implique que no requieran de alguna protección física. Si bien es cierto que contar con una red inalámbrica requiere un poco más de consideraciones en su administración, las ventajas y bondades que nos ofrece su implementación, bien valen la pena.

Con las recientes innovaciones en Software y Hardware podemos lograr un ambiente que permita a las organizaciones grandes, medianas y pequeñas, cubrir sus necesidades de seguridad, sin perder de vista a que los usuarios lleven a cabo sus labores del día a día y que además le brinden la oportunidad de generar y ofrecer soluciones innovadoras que ayuden a

ser un diferenciador en los procesos de negocios de las mismas.

A lo largo del tiempo, Intel ha desarrollado diversas tecnologías que han ayudado a mejorar la facilidad de uso y la seguridad en los ambientes inalámbricos. Desde el lanzamiento de la plataforma Centrino, Intel se ha preocupado en ofrecer, en conjunto con los líderes de la industria de seguridad, soluciones y opciones que permitan encontrar una alternativa acorde a las necesidades de cada empresa. Siguiendo en el camino de innovación, Intel ha desarrollado Intel AMT (Active Management Technology) para ofrecer nuevas soluciones en ambientes de redes alámbricas, facilitando y ayudando en la administración de la PC, mejorando la administración de la misma. Dicha tecnología ayuda a reducir los tiempos por sistemas caídos, reduce las visitas en sitio para diagnósticos y reparación de los problemas más comunes, ayudando en las tareas de administración, sin perder por ello la parte de desempeño, punto importante para los usuarios.

JFS

Con esta nueva innovación en administración, Intel ofrece en el mercado la nueva plataforma vPro que ayuda desde la pequeña empresa (donde al no contar con un área de TI, cada interrupción o caída del sistema implica un alto costo en tiempo y dinero). En el ambiente de las empresas medianas y grandes, apoya al departamento de TI a mejorar la seguridad y la administración.

Las ventajas de vPro están enfocadas a una administración, sin importar si el equipo está apagado o el estado del sistema operativo, permitiendo llevar a cabo operaciones fuera de los horarios de oficina, tales como respaldos de información, actualizaciones de BIOS, defragmentación de discos, actualización e instalación de parches y algunas otras tareas de administración, como puede ser el inventario de los equipos de forma remota, reduciendo las fallas de los procesos manuales.

En el tema de seguridad, la plataforma está enfocada en la seguridad proactiva, habilitando ambientes donde se detecte cualquier variación en la seguridad, como deshabilitar un agente o inhibir la ejecución de un antivirus, clásicos ataques y huecos de seguridad, llevando a cabo acciones preventivas y correctivas, como puede ser que se desconecte de forma automática de la red sin perder sus capacidades de ser administrada o monitoreada.

Al reducirse las acciones por atención en sitio, se contribuye con la reducción en los costos de soporte, se mejora la eficiencia del personal de TI y se incrementa la calidad del servicio, tanto a clientes internos como externos.

La seguridad no sólo implica los procesos físicos, sino que también deben considerarse los procesos de negocio. En los negocios, como en la vida, la derrota es consecuencia de hacer las cosas y afrontar las consecuencias de enfrentar la posibilidad de fallar o bien no hacer nada y claudicar al fracaso como inminente resultado de no hacer nada.

Manejo seguro de correo electrónico

Por Juan Francisco Serrano
Director General
Joint Future Systems

A nivel mundial, cada vez es más común el uso de correo electrónico para comunicar desde la información más trivial hasta negocios multimillonarios. Sin embargo, la mayoría de los usuarios desconoce reglas elementales de seguridad en sus comunicaciones, y muy pocos llegan a grados aceptables de seguridad en su correo.

Existen varias condiciones que deben existir al utilizar correo electrónico. De manera general son las siguientes:

- Asegurar que pueda ser enviado / recibido de manera consistente y confiable.
- Asegurar que sólo pueda ser leído por las personas a las que sea dirigido.
- Asegurar que haya integridad en la información, es decir, que no haya sido modificada.
- Asegurar que, en efecto, haya sido enviado por la persona que aparenta ser.

En los tiempos actuales, existen una serie de amenazas al correo electrónico. Entre otros: incluyen:

Phishing / Pharming: correos enviados por personas que buscan que el que recibe el correo divulgue información confidencial, de diversas maneras.
Virus: correos que contienen archivos de diferentes tipos, que buscan hacer algún daño en el equipo que lo recibe, o que permiten que otra persona se apodere de él.
Spam: Correo no solicitado, que hace que el usuario pierda tiempo al revisarlo.
Spyware: Correos que contienen programas que registran todo lo que hace un usuario en una computadora, (por ejemplo las teclas que oprime o las pantallas que ve), y envía la información a otra persona.

Existen diversos programas que el usuario puede instalar en su computadora para evitar este tipo de ataques, los cuales son más frecuentes en equipos que corren sistemas operativos comerciales, aunque existen en casi todos los sistemas operativos. Lo importante es que el usuario conozca los peligros inherentes al sistema que utilice y que se asegure de tener protección adecuada. En general, se requiere un grupo de programas para controlar los diferentes tipos de amenazas, cada uno con una función específica.

Por otra parte, los correos electrónicos, sobre todo en el ámbito empresarial, pueden ser vulnerables a que información confidencial sea transmitida por ellos, de manera no autorizada (accidentalmente o por mala intención del personal). Para evitar esto, se recomienda instalar programas que controlen el contenido, que impongan candados para que se revise todo documento saliente de manera automática y que, de acuerdo a palabras claves, fecha, hora, u otros factores definidos por el administrador del sistema, evite que un documento con determinadas características sea enviado por una persona que no tiene autorización para hacerlo.

Para aumentar el nivel de seguridad de correo, se utilizan diversas formas de encripción, en la cual la información es codificada de determinada manera, enviada y decodificada por el receptor. Una forma muy popular, y que se integra con muchos de los programas de correo más populares, es PGP. El acrónimo significa Pretty Good Privacy y es una solución 100% de software. Existen múltiples tipos de encripción vía software en el mercado, de diferentes capacidades, precios, y características. Si el usuario quiere soluciones más robustas, puede utilizar equipos (hardware) que están diseñados específicamente para encriptar y desencriptar información. En este caso, tanto el receptor como el emisor tienen que tener equipo compatible entre ellos. En extremos de confidencialidad, la información del correo electrónico no se teclea en la computadora directamente y nunca se despliega en pantalla, sino que es capturada mediante un equipo especial (que combina un escáner con un encriptador), para que la información esté protegida inclusive antes

de que pase al programa de correo. Del otro lado se sigue un proceso inverso, en donde se imprime la información y desencripta fuera de la computadora.

El grado de protección que un usuario requiere para su correo debe ir de acuerdo a lo confidencial de la información que maneje. Los requisitos de seguridad de un usuario casero generalmente son diferentes de los de un usuario corporativo, y también no es lo mismo el grado de seguridad que debe tener un equipo en el cual se hacen regularmente operaciones sensibles como por ejemplo transacciones bancarias, que el que requiere un equipo que se usa principalmente para jugar o hacer trabajos escolares.

JFS

Los correos gratuitos en general no ofrecen grandes niveles de seguridad, (aunque se pueden modificar en algunos casos para ofrecer más garantías). En el caso de los más populares, se requiere pasar a versiones pagadas, para tener un nivel más adecuado de seguridad y privacidad. Se puede inclusive solicitar al proveedor de correo que maneje un nivel determinado de seguridad, acordado en un SLA (Service Level Agreement, o Acuerdo de Nivel de Servicio), el cual varía en costo de acuerdo a la cantidad de candados y protecciones que ofrezca.

Un elemento de seguridad que es bastante efectivo, es el uso de "listas blancas". Esto consiste en configurar el correo de tal manera que sólo recibe correos de cuentas que están pre-autorizadas por el usuario. En el modelo más cerrado, todo correo proveniente de un emisor que no esté autorizado es rechazado automáticamente. En un modelo más abierto, el receptor recibe un correo que indica que el emisor ha tratado de enviarle un mensaje y pide autorización para incluirlo en la lista de emisores autorizados. Esto puede significar complejidades para personas u organizaciones que de manera rutinaria pueden recibir correos de direcciones que no conocen (clientes nuevos, solicitudes de información, etc.).

Independientemente del ámbito en el que se utilice el correo electrónico, deben existir siempre una serie de procedimientos para minimizar los riesgos. A continuación se presentan una serie de recomendaciones generales:

1. Manejar listas blancas para correos muy importantes.
2. Tener los programas actualizados, (sistema operativo, antivirus, parches, versiones) y contar con los programas preventivos instalados.
3. Tener varias cuentas de correo, para diferentes usos. Por ejemplo, una cuenta chatarra que se use únicamente para registro a sitios de Internet que lo requieran.
4. No compartir nunca las claves de correo electrónico con nadie, y cambiarlas frecuentemente.
5. Evitar mandar correos con listas de receptores de manera que todas las personas que leen el correo puedan ver a todos los demás, a menos que esto sea específicamente lo que se está buscando. Esto se logra mediante las funciones de copias ocultas (Bcc y cco, por ejemplo).
6. No participar en cadenas de correo, y evitar reenviar correos de manera indiscriminada.
7. Evitar que haya un uso indiscriminado de correo en máquinas que se utilicen para cuestiones sensibles, como manejo de bancos.
8. Consultar con un experto para obtener un nivel de protección adecuado, de acuerdo al uso que se le dé al equipo.
9. No utilizar cuentas de correo en donde usualmente se maneje información altamente confidencial, en equipos públicos (cafés Internet, aeropuertos, etc.).

Aunque estas recomendaciones ayudan, es importante recordar que ni el correo electrónico, ni Internet, fueron creados de inicio como medios seguros. Se ha avanzado mucho en la materia, pero no existe un sistema 100% seguro en correo electrónico.

El correo electrónico es uno de los medios para comunicarse más efectivos a nivel mundial y se está extendiendo a equipos portátiles, (incluyendo PDAs, teléfonos, televisión, y hasta automóviles). En los próximos años veremos avances muy interesantes y sabemos que la seguridad en este tema seguirá siendo un reto y una oportunidad para todos los usuarios.

Gestión de Identidad de Usuarios. . . "Elemento crítico a considerar en una estrategia de seguridad corporativa"

Por Gerardo Sánchez A.
Presidente
QoS Labs de México

La realidad de las organizaciones es la constante dificultad que se presenta para desarrollar estrategias más eficientes relacionadas a la administración y control de accesos internos y externos de usuarios a los recursos corporativos, al acceso personalizado de los mismos, al manejo de información confidencial, así como al cumplimiento adecuado de las normas regulatorias, que requiere de un estricto control interno y de un alto nivel de seguridad.

La Gestión de Identidad o Identity Management (IDM), provee a las empresas una solución de negocios que resuelve el problema de "aprovisionar" y "desaprovisionar" empleados con acceso a los recursos corporativos (aplicaciones, servicios e instalaciones), y mantener rastro de su actividad en los sistemas, así como de los documentos y de las tareas de procesos y proyectos relacionados a los mismos.

Implementar una solución de IDM, ayuda a las empresas a gestionar en tiempo real los accesos de sus empleados a los recursos corporativos, con una mayor efectividad y a un menor costo, a lo largo de su permanencia en la empresa.

La gestión de identidades se ha convertido en un tema crítico para aquellas empresas donde es muy importante la administración de accesos de un número considerable de usuarios (empleados, socios de negocio, proveedores y consumidores) y un amplio rango de recursos y servicios, incluyendo instalaciones, aplicaciones distribuidas, servicios de red, bases de datos y servicios de intranet/extranet.

Las nuevas regulaciones en materia de seguridad financiera que han surgido en los últimos años, obligan a las compañías a modernizar sus sistemas de seguridad financiera para cumplir con ciertos estándares, contar con información de registro de usuarios en "tiempo real" o bien, en periodos que no excedan las 48 horas; mantener políticas adecuadas para la detección y corrección de violaciones de acceso entre otras (ej: ley Sarbanes-Oxley).

Para facilitar su entendimiento, los beneficios para clientes al implementar una solución IDM fueron divididos en tres grandes rubros:

- Incremento de la productividad y del ingreso:
  - Hacer productivos más rápidamente a los empleados de reciente ingreso, habilitando sus servicios en horas y no semanas.
  - Acceso a recursos corporativos adicionales (aplicaciones, servicios y/o instalaciones) más rápidamente.
  - Liberación acelerada de nuevos servicios web.
  - Reducción de la complejidad de acceso a aplicaciones a través de single sign-on en web.
- Mejora la seguridad:
  - Aquellos empleados que se separen de la organización, son "desaprovisionados" del ambiente de forma rápida y automática.
  - Mejora y auxilia el cumplimiento regulatorio (FERPA, HIPAA y Sarbanes-Oxley).
  - Reduce los riesgos de seguridad o la pérdida de activos al proveer una arquitectura consistente, segura y escalable, centralizando el control de accesos, la autenticación y autorización de usuarios.

- Implantación de actividades "anti-fraude" con procesos bien establecidos, incluyendo responsabilidad de seguimiento para cada una de las partes involucradas, así como criterios para su solución.
- Mejora en la definición de controles, así como de la relación entre controles y riesgos, a lo largo de la organización.

- Reduce costos y mejora la eficiencia operacional:

  - Reduce llamadas al Call Center (por ejemplo, renovación de contraseña automáticamente).
  - Mejora la certeza y precisión de los datos al reducir la cantidad de veces que se debe ingresar información en múltiples sistemas.
  - No requiere de la sustitución de infraestructura y software ("rip and replace").
  - Reduce el tiempo y la complejidad que se requiere para administrar cuentas (tareas de administración con integración a los procesos de Recursos Humanos, suministro y desaprovisionamiento de cuentas, modificaciones en los perfiles y roles de usuarios, cambio o regeneración de las claves de seguridad, administración de información personal, etc.).

Conociendo los beneficios ofrecidos por este tipo de soluciones, es importante dar a conocer las características que deben cubrir las empresas que mejor capitalizarán este tipo de tecnologías, en el corto plazo.

- Contar con al menos 800 cuentas de usuarios administradas.
- Alto requerimiento de servicios de TI para usuarios (más de 3 aplicaciones/servicios).
- Contar con algún sistema ERP/HRMS ya implementado.
- Usuarios con un promedio de tres cuentas de acceso a aplicaciones.
- Alto uso de personal externo con requerimientos de acceso a recursos corporativos restringidos (consultores, agentes, proveedores, etc.).
- Alto uso de personal temporal con requerimientos de acceso a recursos corporativos restringidos (por proyectos, por temporada, etc.).
- Se encuentren en proyectos para cumplir con regulaciones gubernamentales.
- Se encuentren disminuyendo costos administrativos o buscando optimización de sus procesos operativos.

En caso de evaluar una solución de gestión de identidad de usuarios, recomendamos a las empresas considerar lo siguientes puntos:

- Que la solución sea altamente modular, escalable, extensible e integrable, permitiendo una rápida integración y con esto una considerable reducción de costos. Solución de desarrollo acelerado y rápida implantación.
- Arquitectura abierta y compatible con los principales estándares de la industria (por ejemplo, SPML y LDAP).
- Solución basada en una arquitectura orientada a servicios (SOA) que permite establecer lineamientos claros de desarrollo e integración de componentes al ambiente de TI, permitiendo capitalizar los beneficios que este tipo de arquitectura brinda: re-usable, compartible, confiable, segura y robusta.
- Que el proveedor cuente con el respaldo de una base instalada de clientes.
- Que sea flexible, de forma tal, que pueda adecuarse a los requerimientos de sus clientes.
- Solidez en la funcionalidad de sus conectores y en el módulo de administración de políticas de acceso e identidad.
- Que cuente con una completa funcionalidad de auditoría de identidad. Indispensable en proyectos de cumplimiento regulatorio.

Las tecnologías de información, en particular aquéllas relacionadas a arquitecturas orientadas a servicio (SOA), como lo es la Gestión de Identidades, representan una herramienta poderosa para apoyar y asegurar un manejo adecuado, seguro, rastreable y eficaz de los distintos usuarios que interactúan con las organizaciones que, por su dinámica organizacional, así lo requieran y justifiquen.

Para mayor información, visite:
http://soluciones-soa.qoslabs.com o
escríbanos a soluciones-soa@qoslabs.com

Habilitando la Empresa Virtual
Un nuevo paradigma empresarial.
La era de la participación.

Por Paulo Kalapis
Director de Software Marketing para América Latina
Sun Microsystems México.

La era de la participación está introduciendo una nueva era en el crecimiento y la oportunidad de negocios. Alrededor nuestro, en la empresa, en la comunidad de desarrolladores, entre las empresas y los consumidores y en el sector público, las personas se encuentran interactuando y colaborando de una manera que hace unos pocos años era imposible. Esta nueva forma de interactuar se define como el nuevo Web 2.0. Estas nuevas posibilidades han creado rápidamente nuevas expectativas para la empresa de hoy.

La red se está volviendo el nexo de enlace para cada vez más usuarios. A medida que crece la necesidad por servicios en línea, surge un nuevo conjunto de necesidades tanto para los usuarios como para las empresas:

- Las expectativas de los usuarios de más alternativas, junto con mejores contenidos y servicios, continuarán en aumento.
- Las empresas están ansiosas por cumplir con esas expectativas, poniendo a disposición más aplicaciones y servicios.
- Las presiones de la competencia impulsan a las empresas a generar nuevas líneas de ingresos y nuevos clientes a través de la pronta provisión de nuevos servicios.
- Las empresas deben centrarse también en mantener contenta y leal a la base de clientes actual, mejorando las ofertas de servicios existentes y brindando una excelente experiencia al cliente.

En conjunto, la era de la participación presenta un nuevo paradigma para la manera en que las personas despliegan, acceden y utilizan información, aplicaciones y recursos en red. Las barreras de acceso deben caer, liberando a los usuarios y las empresas para que lleven la experiencia en línea hasta los límites conocidos y aún más allá.

Este cambio trae tremendas oportunidades para las empresas, aunque también requiere acceso general, en el cual la identidad del usuario es un factor facilitador imprescindible. Después de todo, la participación requiere confianza. Y la confianza requiere identidad. En la actualidad, existe una necesidad innegable y urgente de las empresas y los individuos para saber quién está del otro lado de sus transacciones, para confiar en esa entidad y tener la seguridad de que la información que comparten con ellos está segura. La gestión de identidades tiene todas las respuestas a estas necesidades y se vuelve el factor facilitador de la era de la participación.

Mediante la provisión de todo lo necesario para gestionar las identidades de manera efectiva, tanto dentro de la empresa como en los límites de los negocios tradicionales, la gestión de identidades hace posible proveer de manera segura los recursos correctos a las personas adecuadas en el momento y contexto que corresponde. De esta manera, puede permitir que las empresas aceleren enormemente el crecimiento a la vez que dejan a sus competidores en el camino, y lo hacen de manera segura y a salvo.

Para mayor información, visite:
http://www.sun.com/software
o escríbanos a soa-la@sun.com

Consejos para mejorar las entregas y aperturas, utilizando buenas prácticas para el correo electrónico

Extracto de TRALiX whitepaper, proporcionado por
Enrique Gómez Moya
Director Comercial
Tralix

INTRODUCCIÓN

Día con día, los Proveedores de Servicios de Internet (ISP's) y los Proveedores de Correo Electrónico, evolucionan y crean nuevas técnicas para disminuir el SPAM en las bandejas de entrada.

Debido a lo anterior, quienes integramos el email en nuestro proceso de negocios, debemos poner especial énfasis para que nuestros mensajes no sean erróneamente confundidos como correo no deseado.

El primer obstáculo corresponde a la capacidad de que nuestros emails sean correctamente recibidos (deliverability).

El segundo obstáculo se refiere a lograr que nuestros emails no sean catalogados como SPAM.

LOGRAR EMAILS CORRECTAMENTE ENTREGADOS.

A pesar de que cada dominio de correo electrónico está regulado y configurado de manera distinta, y de que en muchas ocasiones es necesario hacer ajustes especiales para realizar o mejorar las entregas, existen diversas prácticas que se deben seguir de manera general para asegurar el éxito en esta fase.

Práctica No.1:
NO APARECER EN LOS DNSBL.

Un mecanismo muy común y fácil de implementar por los ISP's y proveedores de email para reducir el correo no deseado, es la verificación de la dirección IP de origen, es decir, las llamadas DNS blacklist (DNSBL).

Los servicios de Black Listing más usados son:

The Spamhaus Block List
http://www.spamhaus.org/sbl/index.lasso

SORBS
http://www.us.sorbs.net/lookup.shtml

Multi-RBL Check
http://www.robtex.com/rbls.html

Práctica No. 2:
PERTENECER A PROGRAMAS DE WHITELIST

De la misma manera que existen listas negativas para bloquear los envíos, existen las "listas blancas" (whitelist).

Entre los programas y tecnologías de Whitelistening más destacados están:

- AOL Whitelist
- Prodigy México Whitelist
- Domain Keys
- Sender Policy Framework

Práctica No. 3:
EVITAR EL EMAIL FORGERY

Email forgery o robo de identidad de email, es cuando se falsifica la identidad de quien envía un email, muchas veces con la intención de engañar al destinatario y obtener información confidencial de forma fraudulenta (práctica conocida en el ámbito informática con el término de phishing).

Debemos tener particular cuidado al crear o elegir la configuración de envío con características con los cuales los emails son enviados. El error más común es usar un remitente (from) correspondiente al dominio, sin la configuración adecuada.

Práctica 4:
TRATAMIENTO EFICAZ DE LOS BOUNCES

Un bounce es la contestación automática de que un email no pudo ser entregado de forma exitosa. Existen muchas razones por las cuales un email no pudo ser entregado; dependiendo de este motivo, se cataloga un bounce como un hard-bounce o un soft-bounce.

Un hard-bounce suele ser cuando la dirección de email en cuestión está escrita incorrectamente o simplemente ya no existe; un soft-bounce usualmente está ligado a un problema en el servidor destino (espacio lleno, muchas conexiones, etc), o puede ser que haya sido rechazado por un filtro Anti-SPAM.

También es importante monitorear constantemente las quejas y peticiones de de-suscripción que regresen como contestaciones (replies), por medio del correo de regreso de los usuarios.

Debemos evitar a toda costa la reactivación de emails que hayan sido de-suscritos por hard-bounces, así como tener especial cuidado en importar correctamente nuevos clientes a nuestras audiencias.

Práctica 5:
PUBLICAR LAS POLÍTICAS DE PRIVACIDAD Y ENVÍO DE CORREOS

Publicar y RESPETAR las políticas de privacidad y de AntiSpam, como las siguientes:

http://www.tralix.com.mx/privacy.html
http://www.tralix.com.mx/antispam.html

Práctica 6:
CONTAR CON POLÍTICAS DE SATURACIÓN

Estas políticas tienen que ver con la frecuencia que se contactará al usuario a lo largo del tiempo, donde en el mejor de los casos el Usuario nos "dirá" con qué frecuencia desea se contactado por los comunicados que le enviemos.

LOGRAR QUE LOS EMAILS LLEGUEN A LA BANDEJA DE ENTRADA

Algo importante que se debe comprender, es que el hecho de que un email haya sido correctamente recibido por el servidor de correo, de ninguna manera garantiza que éste llegará a la bandeja de entrada del usuario.

Esto se debe a que en la actualidad prácticamente todos los programas de email y sistemas de email basados en WEB, cuentan con filtros anti-SPAM.

Práctica 7:
NO CREAR CORREOS QUE PAREZCAN SPAM

Entre las recomendaciones más comunes a seguir, se encuentran las siguientes:

- Evitar el uso de imágenes muy grandes.
- Evitar el uso de textos con tamaño de letra muy pequeña o muy grande.
- Evitar el uso de textos CoMo EsTe.
- Evitar el uso de E.S.P.A.C.I.O.S en las palabras
- Evitar el uso de |etras extr@ñas o num3r0s.
- Aplicación de criterios del mantenimiento y actualización de la base de datos.
- Aplicación de criterios de uso de ligas de re-direccionamiento.
- Aplicación de criterios de uso de espacios de comercialización.
- Aplicación de criterios de diseño de piezas HTML.
- Usar herramientas que generen buen HTML.
- No usar colores para texto que se pueda confundir con el color de fondo.
- Tamaño de las piezas de Correo.
- Uso de archivos anexos y aplicaciones enriquecidas.
- Evitar en medida de lo posible las siguientes palabras (y sus variaciones y traducciones)

- Offer
- Viagra
- Rolex
- Mortage
- Sex
- Porn

Práctica 8:
EVITAR LOS FILTROS DE USUARIO

Los filtros de usuario son el último obstáculo para que el email llegue a la bandeja de entrada. Los filtros de usuario pueden ser positivos (en el caso de las listas de contacto) o negativos (en el caso de las listas de bloqueo) y por su naturaleza ni el Sender más avanzado, ni los mejores programas de whitelist o tecnología de certificación, pueden modificar éstos valores.

JFS

De acuerdo con un estudio realizado por TRUSTe[1] y Epsilon[2] en Octubre del 2006, en la actualidad los consumidores están acostumbrados a calificar como SPAM a cualquier correo que no le sea relevante, no recuerden claramente haberlo solicitado o les parezca sospechoso. A esto le sumamos la integración de los botones de "Report SPAM" que los clientes de correo más importantes han añadido en los últimos meses.

Para evitar los filtros del usuario, usted puede agregar una liga de "Agréganos" a su email, la cual muestra una página preparada donde se dan instrucciones detalladas sobre cómo agregar la dirección del from a la agenda de direcciones de diversos clientes de correo electrónico.

Recuerde, nadie es inmune a cualquier comunicación masiva por email.

LOGRAR QUE LOS EMAILS SEAN ABIERTOS

Una vez que un email ha sido depositado en la bandeja de entrada del cliente, es cuando el asunto del correo electrónico (subject) y el contenido del mensaje juegan el papel más importante.

Práctica 9:
CONSIDERE LA HORA Y FECHA DEL ENVÍO

- No realice su envío los viernes por la tarde.
- Considere que los envíos que realice por la tarde o noche serán abiertos en su mayoría al siguiente día.
- Las bandejas de entrada suelen saturarse de promociones en la temporada navideña.

Práctica 10:
USE SUBJECTS ADECUADOS

- Cree más de un subject para sus envíos y envíe al más exitoso.
- No use subjects trillados como "Ofertas de fin de temporada" o "Última oportunidad".
- De ser posible, use algún campo de personalización en el subject.

Práctica 11:
CUIDE EL CONTENIDO DE SU CORREO

- Entre más focalizado sea el correo, mejor respuesta tendrá.
- No use mensaje enriquecido a menos que su audiencia realmente lo requiera.

Para cualquier comentario estaremos felices de atenderlos en customercare@tralix.com.

[1] http://www.truste.org [2] http://www.epsilon.com