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

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

Deutsch-Mexikanische
Industrie- und Handelskammer
Cámara Mexicano-Alemana
de Comercio e Industria | CAMEXA

ESTUDIO DE PERCEPCIÓN
SEGURIDAD DE LA INFORMACIÓN MÉXICO 2009

La dinámica mundial en la investigación y desarrollo de productos, así como en la configuración de reglas que permiten fortalecer la seguridad de la información, mantiene un ritmo acelerado. Año con año surgen nuevos estándares, se actualizan los existentes, se fabrica más y mejor tecnología encaminada a la protección de datos y a la ampliación de los rangos de disponibilidad de los servicios. La seguridad de la información, lejos de perder importancia, se vuelve, cada vez más, un aspecto fundamental en todos los ámbitos: en el intercambio de ideas y conocimientos, en las relaciones de negocios, en el día a día a nivel personal y empresarial. Las grandes organizaciones del mundo están más cerca de la implementación y el refinamiento de sus procesos, fortalecen la infraestructura de sus redes e incorporan procedimientos de acceso y manejo de información cada vez más rigurosos; pero, ¿Qué está sucediendo en México? ¿Cuál es la percepción de los usuarios de tecnología alrededor del tema? ¿Qué tanto ha permeado una cultura de Seguridad de la Información en nuestro país?

El Estudio de Percepción sobre Seguridad de la Información en México que se lleva a cabo desde 2004, tiene como propósito responder a estas preguntas y servir como "termómetro" de lo que al respecto se piensa, y se conoce, entre los usuarios especializados y no especializados, en el ámbito organizacional.

Con el propósito de brindar un panorama lo más completo posible respecto del tema, se ha recopilado información y opiniones de diferentes fuentes, obteniendo así la percepción del trabajador convencional (No-Informático) y del trabajador cercano a la tecnología (Informático), así como la opinión experta de quienes lideran áreas ligadas de manera muy directa a la seguridad de la información y de los sistemas en sus organizaciones. Por tal razón, este documento se conforma de 3 secciones complementarias:

A. Encuesta entre usuarios de diferentes áreas organizacionales, tanto de empresas privadas como de instituciones públicas.

B. Estudio de opinión y análisis con 18 expertos en temas relacionados con seguridad en informática.

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

JFS

KIO Networks

Secure Information Technologies

Universidad Iberoamericana Ciudad de México

CONTENIDO

I. ALCANCES DE LA INVESTIGACIÓN TOTAL 6

II. INVESTIGACIÓN ENTRE EMPRESAS Y ÁREAS USUARIAS DE TI 7

OBJETIVOS DEL ESTUDIO 7
METODOLOGÍA 7
- Método de investigación 7
- Características de la muestra 7
  - Perfil de los entrevistados 7
  - Tamaño de la muestra 7
- Codificación de respuestas 8

RESULTADOS 9
- Composición de la muestra 9
- Qué se entiende por "Seguridad en Informática" 10
- Principales preocupaciones acerca de la Seguridad de equipos de cómputo y su contenido. 12
- Amenazas de mayor riesgo para la Seguridad de la Información. 13
- Normas y regulaciones de seguridad que conoce 14
- Qué hace falta por parte de los proveedores de TI 15
- Importancia de la Seguridad en Informática en las empresas 16
- Aspectos a tomar en cuenta en la compra de tecnología 17
- Percepción acerca de diversas marcas asociadas con Seguridad en Informática 18
- Qué más les gustaría conocer acerca de Seguridad en Informática 20

III.ESTUDIO CON EXPERTOS Y PROVEEDORES LÍDERES DEL MERCADO TI 22

OBJETIVOS DEL ESTUDIO 22
METODOLOGÍA 22
Método de investigación 22
RESULTADOS 23
Situación de la Seguridad en Informática en México, frente a otros países del mundo 23
Principales retos de México como país, en materia de Seguridad en Informática 25
Impacto que podría tener la situación económica mundial de 2009 en la percepción sobre Seguridad de la Información por parte de la gente 27
Principales retos de las organizaciones usuarias, en materia de Seguridad en Informática 28
Principales retos de los proveedores de hardware y software, en materia de Seguridad en Informática 28
Principales retos de las Instituciones Educativas mexicanas, en materia de Seguridad en Informática 29
Principales retos de los Medios de Comunicación, en materia de Seguridad en Informática 30
Principales retos del Gobierno de México, en materia de Seguridad en Informática 31
APORTACIONES RELACIONADAS CON SEGURIDAD EN INFORMÁTICA, HECHAS POR LAS EMPRESAS ENTREVISTADAS 32

IV. CONCLUSIONES DE LA INVESTIGACIÓN 34

AVANCES IMPORTANTES EN 2009 34
ASPECTOS QUE SIGUEN REZAGADOS 34

V. ARTÍCULOS SOBRE SEGURIDAD EN INFORMÁTICA 35

ALAPSI FRENTE AL ESTUDIO DE PERCEPCIÓN DE SEGURIDAD 2009 35
SEGURIDAD: EL ORDEN DE LOS FACTORES SÍ ALTERA EL PRODUCTO 37
EL CAMBIANTE PERFIL DEL "HACKER" 39
LOS RIESGOS DE LAS REDES SOCIALES 41
GESTIÓN DE RIESGOS DE TI UTILIZANDO ISO31000 E ISO27005 43
HACIA UNA CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN 46

JFS KIO Networks Secure Information Technologies Universidad Iberoamericana Ciudad de México

I. ALCANCES DE LA INVESTIGACIÓN TOTAL

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

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

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

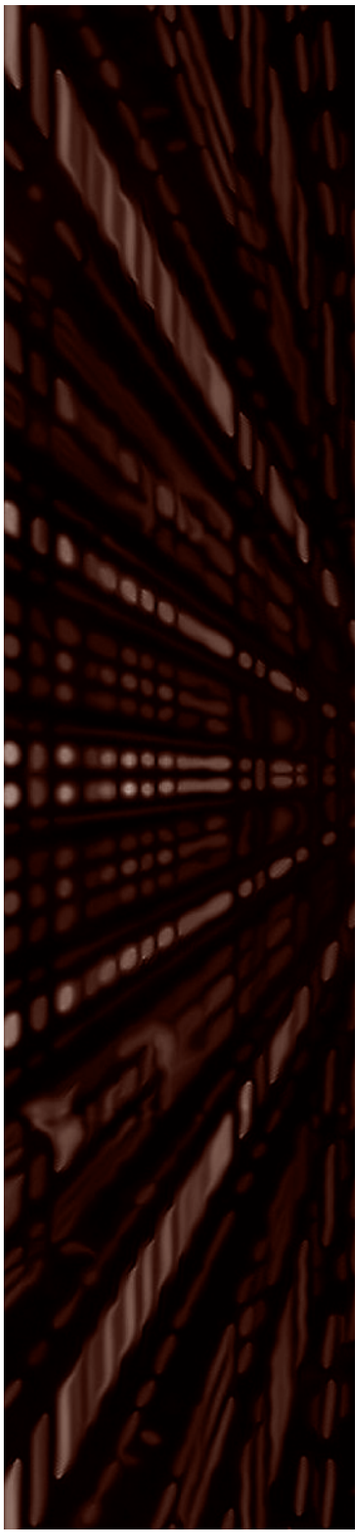
4. Conocer la percepción que tienen diferentes expertos y algunos proveedores cuyas soluciones tienen incidencia directa o indirecta sobre la Seguridad en Informática, respecto del grado de conocimientos y penetración de esta cultura entre las organizaciones de nuestro país.

5. Conocer cuáles normas y regulaciones relacionadas con seguridad en informática están presentes en la mente de los usuarios en general.

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

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

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



II. INVESTIGACIÓN ENTRE EMPRESAS Y ÁREAS USUARIAS DE TI

OBJETIVOS DEL ESTUDIO

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

METODOLOGÍA

Método de investigación

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

Posteriormente, se realizaron encuestas complementarias que permitieron cubrir la cuota de 250 entrevistados de la categoría Informáticos, equivalentes al 22.9 por ciento de la muestra total.

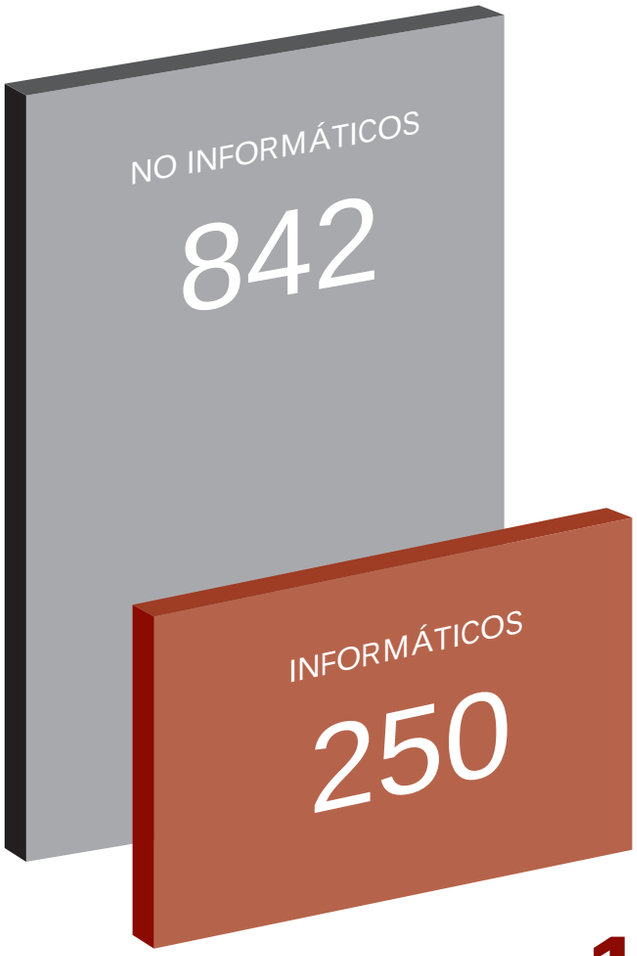
Características de la muestra

Se utilizó una muestra no probabilística, con las siguientes características.

Perfil de los entrevistados

Característica principal	Directivos y niveles medios de diferentes áreas organizacionales, de instituciones y empresas de todos tamaños.
Edad:	Indistinta
Sexo:	Indistinto
Cobertura geográfica:	Múltiple, dentro de la República Mexicana
N.S.E.	Indistinto
Especiales	1.Ser usuario de soluciones informáticas, con al menos 2 años de antigüedad. 2.Utilizar soluciones informáticas un tiempo mínimo de 10 horas semanales.

Tamaño de la muestra



1,092

GRÁFICA 1

Codificación de respuestas

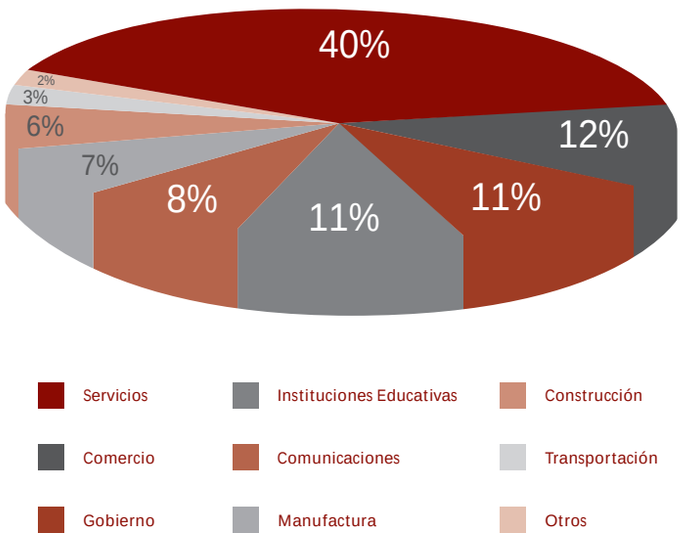
La mayoría de las preguntas solicitaban responder con una selección determinada de respuestas de opción múltiple (las 3 respuestas, principalmente, que resultaran más significativas para el entrevistado, de entre una extensa lista). Para las preguntas que por sus características requerían respuestas abiertas y espontáneas, todas éstas fueron clasificadas en categorías y subcategorías (proceso de codificación) que describen las opiniones de los entrevistados, agrupadas en términos específicos, y que permiten establecer frecuencias y porcentajes.

RESULTADOS

Composición de la muestra

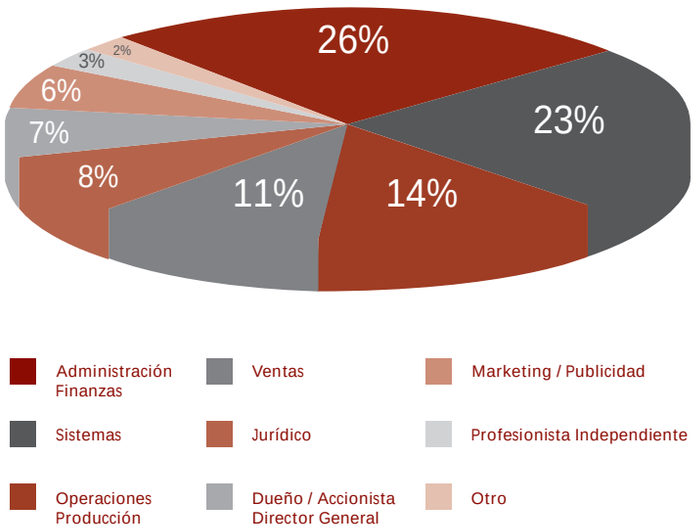
La composición de la muestra se clasifica bajo tres criterios – por sector, por sexo y por puesto o área de trabajo.

Por Sector



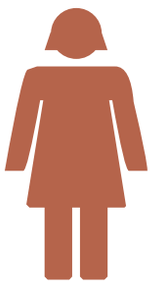
GRÁFICA 2

Por Puesto o Área de Trabajo



GRÁFICA 3

HOMBRES
59%



MUJERES
41%

GRÁFICA 4

Qué se entiende por "Seguridad en Informática"

Pregunta: ¿Para usted qué significa el término "Seguridad en Informática"?

Esta fue una pregunta abierta, lo cual implica que las respuestas de los entrevistados muestran la asociación espontánea del término "Seguridad en Informática" con otros conceptos, mismos que fueron posteriormente codificados en grupos de respuestas similares que derivaron en las categorías que se muestran en la tabla de frecuencias.

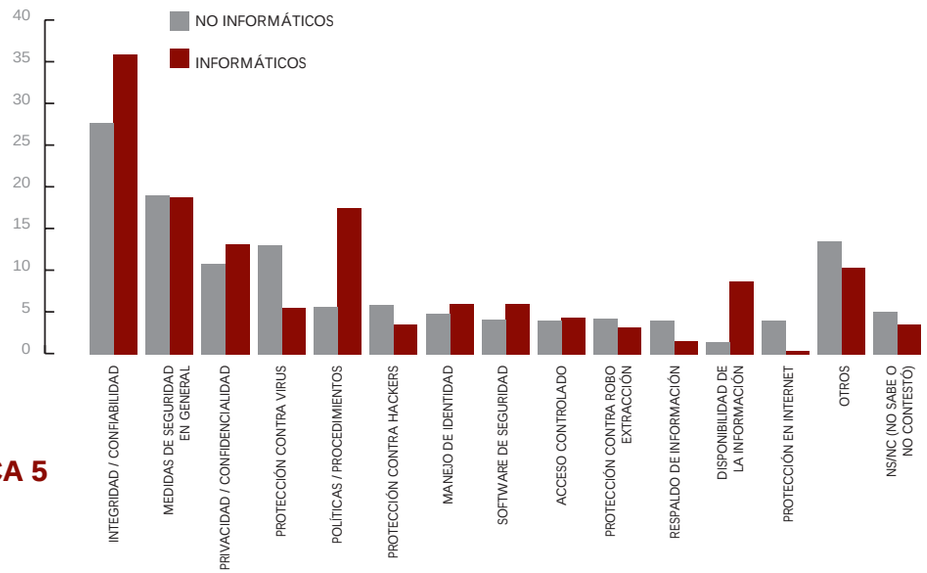
Se registraron todas las respuestas emitidas por los entrevistados, quienes por lo regular mencionaron más de una opción (1.36 respuestas promedio por entrevistado). La frecuencia de las respuestas ya codificadas, puede apreciarse en la Tabla 1 y la Gráfica 5.

TABLA 1

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
Integridad / Confiabilidad de la información	233	27,7%	90	36,0%	323	29,6%
Medidas de seguridad en general	161	19,1%	47	18,8%	208	19,0%
Privacidad / confidencialidad	91	10,8%	33	13,2%	124	11,4%
Protección contra VIRUS	110	13,1%	14	5,6%	124	11,4%
Políticas / procedimientos / uso responsable	48	5,7%	44	17,6%	92	8,4%
Protección contra HACKERS	50	5,9%	9	3,6%	59	5,4%
Manejo de identidad	41	4,9%	15	6,0%	56	5,1%
Software de seguridad	35	4,2%	15	6,0%	50	4,6%
Acceso controlado	34	4,0%	11	4,4%	45	4,1%
Protección contra ROBO / EXTRACCIÓN	36	4,3%	8	3,2%	44	4,0%
Respaldo de información	34	4,0%	4	1,6%	35	3,2%
Disponibilidad de la información	13	1,5%	22	8,8%	38	3,5%
Protección en INTERNET	34	4,0%	1	0,4%	35	3,2%
Cuidado de los equipos	25	3,0%	2	0,8%	27	2,5%
Transmisión de datos / comunicaciones seguras	21	2,5%	5	2,0%	26	2,4%
Trabajar con confianza	20	2,4%	3	1,2%	23	2,1%
Hardware de seguridad	10	1,2%	8	3,2%	18	1,6%
Operaciones bancarias o de compra-venta seguras	15	1,8%	1	0,4%	16	1,5%
Protección contra Spyware	8	1,0%	2	0,8%	10	0,9%
Monitoreo / vigilancia	5	0,6%	1	0,4%	6	0,5%
Garantía de continuidad en la operación	1	0,1%	3	1,2%	4	0,4%
Legislación sobre el tema	4	0,5%	-	0,0%	4	0,4%
Filtro de contenidos	3	0,4%	-	0,0%	3	0,3%
Protección contra Spam	2	0,2%	1	0,4%	3	0,3%
Otros	10	1,2%	4	1,6%	9	0,8%
NS/NC (No Sabe o No Contestó)	43	5,1%	9	3,6%	52	4,8%

Para ambos grupos de entrevistados, (No-Informáticos e Informáticos), el concepto de "Seguridad en Informática" está relacionado principalmente con cuestiones que tienen que ver con la Integridad de los Datos y Confiabilidad de la Información (27.7% y 36.0% de cada grupo respectivamente). En segundo lugar, mencionaron una gran variedad de medidas de seguridad en general, bajo términos similares a "el resguardo de toda la información y de los sistemas operativos", "la confianza de que la información esté segura y protegida", "Medidas para proteger la información digital", etc.

En 2009 se incrementó significativamente el número de menciones sobre políticas adecuadas, procedimientos y uso responsable de la tecnología



GRÁFICA 5

Si bien el concepto de Privacidad y Confidencialidad de la Información ocupa el tercer orden en la asociación con "Seguridad en Informática" para la muestra total (124 menciones equivalente al 11.4% de las respuestas), cada grupo en lo individual dio mayor frecuencia de menciones a otros conceptos, en cuanto a lo que significa para ellos la Seguridad en Informática. Para los No-Informáticos, el tercer lugar de las menciones giró en torno a la Protección contra Virus (110 menciones, equivalentes al 13.1% de su grupo), mientras que las Políticas adecuadas, los procedimientos y uso responsable de la tecnología, resultaron de mayor relevancia para el grupo de los Informáticos (44 menciones, equivalentes al 17.6% de esta categoría), en el lugar número 3 en la frecuencia de menciones.

Este rubro de Políticas adecuadas, procedimientos y uso responsable, es mucho más tomado en cuenta por los Informáticos que por los No-Informáticos. Cabe hacer notar que en la encuesta de 2009, el número de menciones de este concepto se incrementó significativamente respecto del año anterior, subiendo de 3.6% a 5.7% en el grupo de los No-Informáticos y de 7.7% a 17.6% en el grupo de los Informáticos.

El uso de software original no es un factor relevante para los entrevistados, como elemento de Seguridad de la Información.

Otra diferencia notoria en la percepción de ambos grupos de entrevistados, se da en el rubro de Disponibilidad de la información, mencionada por el 8.8% de los Informáticos y sólo por el 1.5% de los No-Informáticos.

Llama la atención que algunos conceptos que habían sido mencionados en estudios anteriores con cierta frecuencia, disminuyeron significativamente su participación en la encuesta de este año. Tal es el caso de la Protección para garantizar la integridad personal y familiar (0 menciones), Uso de software original (0 menciones), Phishing e Ingeniería Social (1 mención) y Protección a los derechos de autor (1 mención).

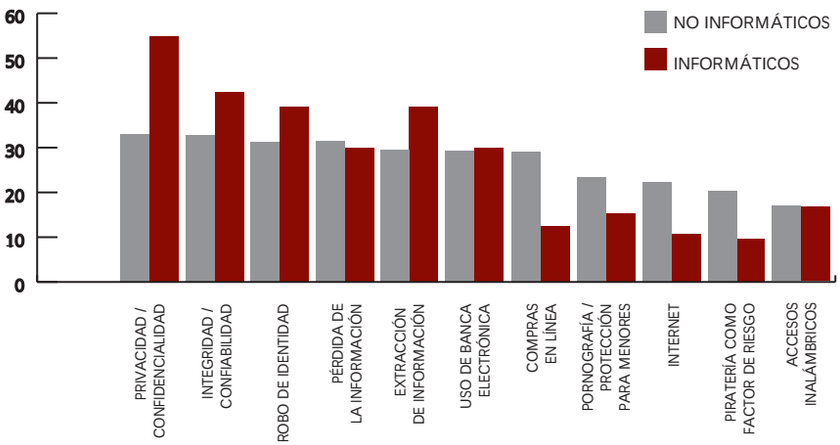
Principales preocupaciones acerca de la Seguridad de equipos de cómputo y su contenido

Pregunta: De la siguiente lista, por favor marque las 3 opciones que representen sus principales preocupaciones en relación con la seguridad de los equipos de cómputo y de su contenido.

TABLA 2

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
Privacidad / Confidencialidad	278	33,0%	137	54,8%	415	38,0%
Integridad / Confiabilidad	276	32,8%	106	42,4%	382	35,0%
Robo de Identidad	263	31,2%	98	39,2%	361	33,1%
Pérdida de la información	273	32,4%	75	30,0%	348	31,9%
Extracción de información	249	29,6%	98	39,2%	347	31,8%
Uso de Banca Electrónica	246	29,2%	75	30,0%	321	29,4%
Compras en línea	245	29,1%	31	12,4%	276	25,3%
Pornografía / protección para menores	196	23,3%	38	15,2%	234	21,4%
Internet	187	22,2%	27	10,8%	214	19,6%
Piratería como factor de riesgo	172	20,4%	24	9,6%	196	17,9%
Accesos Inalámbricos	141	16,7%	41	16,4%	182	16,7%

La Privacidad y Confidencialidad de la Información tiene relevancia para un mayor número de entrevistados (de ambos grupos), sobre la Integridad y la Confiabilidad de la Información (concepto en el según lugar de menciones). Sin embargo, la distancia entre ambos conceptos no es mucha. En definitiva, ambos rubros representan la principal preocupación tanto de No-Informáticos, como de Informáticos.



GRÁFICA 6

Es claro que conceptos como Pornografía y Protección para Menores, las compras en línea, el acceso a Internet en general y la Piratería como factor de riesgo, tienen mayor relevancia para el grupo de los No-Informáticos que para los Informáticos, mientras que para estos últimos, en relación con el otro grupo de entrevistados, la preocupación por conceptos como Privacidad y Confidencialidad de la Información, Integridad y Confiabilidad, Robo de Identidad y Extracción de Información, es mayor.

En cuanto a la Extracción de Información, es notorio que para los entrevistados en 2009 ya no resulta una preocupación tan relevante respecto del estudio del año anterior. Este concepto había ocupado en 2008, la primera posición de menciones (con 64.0% de la muestra total), mientras que este año se colocó en la cuarta posición, con tan sólo un 31.8% de menciones.

Amenazas de mayor riesgo para la Seguridad de la Información

Pregunta: De la siguiente lista, por favor marque las que considere son las 3 amenazas de mayor riesgo para la seguridad de la información.

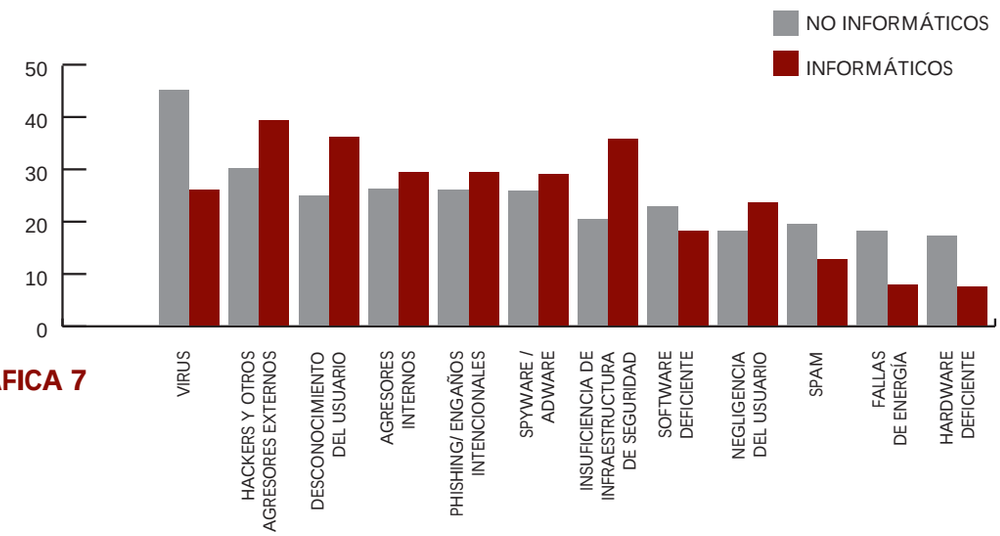
La tabla de frecuencias y gráfica de respuestas a esta pregunta, se presentan, respectivamente, en la Tabla 3 y en la Gráfica 7.

TABLA 3

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
Virus	387	46,0%	66	26,4%	453	41,5%
Hackers y otros agresores externos	259	30,8%	100	40,0%	359	32,9%
Desconocimiento del usuario	214	25,4%	92	36,8%	306	28,0%
Agresores internos	225	26,7%	75	30,0%	300	27,5%
Phishing / Engaños intencionales	223	26,5%	75	30,0%	298	27,3%
Spyware / Adware	222	26,4%	74	29,6%	296	27,1%
Insuficiencia de infraestructura de seguridad	175	20,8%	91	36,4%	266	24,4%
Software Deficiente	196	23,3%	46	18,4%	242	22,2%
Negligencia del usuario	155	18,4%	60	24,0%	215	19,7%
Spam	167	19,8%	32	12,8%	199	18,2%
Fallas de energía	155	18,4%	20	8,0%	175	16,0%
Hardware Deficiente	148	17,6%	19	7,6%	167	15,3%

La amenaza expresada con mayor frecuencia por parte de los No-Informáticos, fueron los Virus, con un 46.0% de menciones de este grupo. En la mayoría de los estudios anteriores, este concepto ha sido la amenaza más significativa para ellos. Sin embargo, para el grupo de los Informáticos este rubro ocupa la séptima posición, con tan sólo un 26.4% de las menciones. La amenaza más mencionada por los Informáticos, fueron los Hackers y agresores externos. Para este último grupo, la amenaza mencionada en segundo lugar es el Desconocimiento de usuario, seguido por una Infraestructura de Seguridad insuficiente. Ambos conceptos detonan alertas especiales en los terrenos de capacitación e inversión.

Después de Virus y Hackers, el "Desconocimiento del usuario" es considerado la tercera amenaza más significativa para los entrevistados (28% de la muestra total).



GRÁFICA 7

Normas y regulaciones de seguridad que conoce

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

La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 4 y en la Gráfica 8.

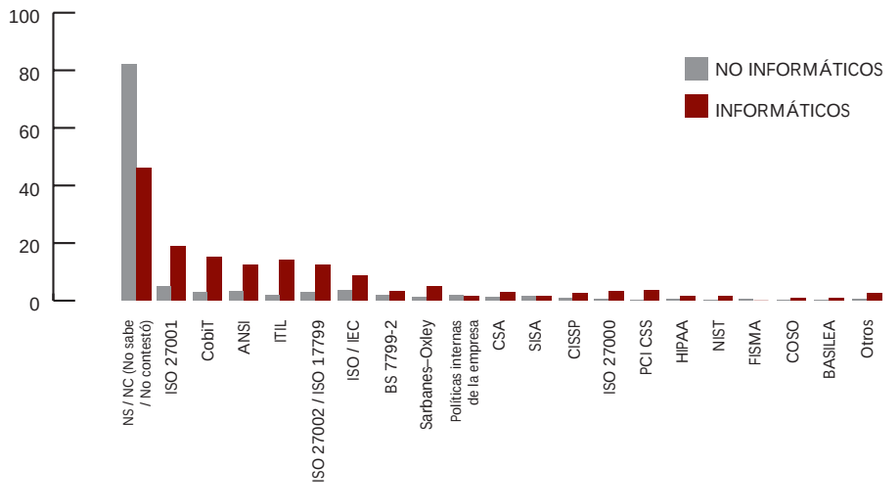
TABLA 4

	No-Informático		Informático		Total	
	x=842		x=250		x=1.092	
NS / NC (No sabe / No contestó)	693	82,3%	115	46,0%	808	74,0%
ISO 27001	40	4,8%	47	18,8%	87	8,0%
CobiT	25	3,0%	38	15,2%	63	5,8%
ANSI	28	3,3%	31	12,4%	59	5,4%
ITIL	24	2,9%	35	14,0%	59	5,4%
ISO 27002 / ISO 17799	25	3,0%	31	12,4%	56	5,1%
ISO / IEC	29	3,4%	22	8,8%	51	4,7%
BS 7799-2	17	2,0%	8	3,2%	25	2,3%
Sarbanes–Oxley	11	1,3%	12	4,8%	23	2,1%
Políticas internas de la empresa	15	1,8%	4	1,6%	19	1,7%
CSA	11	1,3%	7	2,8%	18	1,6%
SISA	13	1,5%	4	1,6%	17	1,6%
CISSP	6	0,7%	6	2,4%	12	1,1%
ISO 27000	4	0,5%	8	3,2%	12	1,1%
PCI CSS	2	0,2%	9	3,6%	11	1,0%
HIPAA	3	0,4%	4	1,6%	7	0,6%
NIST	2	0,2%	4	1,6%	6	0,5%
FISMA	4	0,5%	-	0,0%	4	0,4%
COSO	2	0,2%	2	0,8%	4	0,4%
BASILEA	1	0,1%	2	0,8%	3	0,3%
Otros	4	0,5%	6	2,4%	10	0,9%

Sólo el 17.7% de los No-Informáticos hizo mención de conocer al menos una normatividad enfocada en la seguridad de la información (1.8% mencionaron algún documento de políticas internas de su organización y 15.9% de algún estándar o norma convencional). Destaca significativamente que este porcentaje es muy superior al registrado el año anterior dentro de este grupo de respondentes (únicamente 6.8%), lo cual muestra una mayor efectividad en la difusión de estos conceptos, por un lado, y en el interés de los usuarios por el tema.

74% de los entrevistados, no conoce ningún tipo de política o estándar de Seguridad de la Información.

GRÁFICA 8



En el grupo de los Informáticos, 54.0% (más de la mitad), mencionaron al menos un mecanismo de normatividad o regulación alrededor de la seguridad de la información, lo cual resulta aún más significativo respecto de lo observado en el estudio anterior, en donde sólo 19.3% hicieron alguna mención al respecto.

Qué hace falta por parte de los proveedores de TI

Pregunta: ¿Qué cree usted que deberían mejorar los proveedores de tecnología? Escoja 3 de las siguientes opciones, las que considere más importantes.

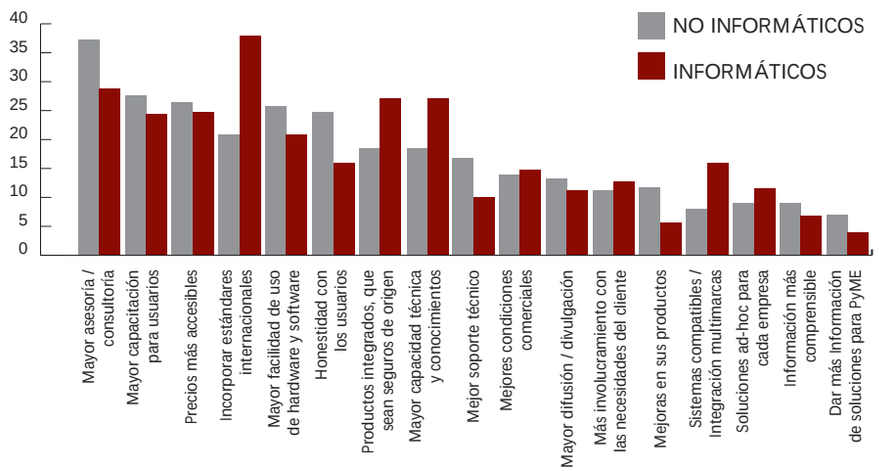
La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 5 y en la Gráfica 9.

TABLA 5

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
Mayor asesoría / consultoría	314	37,3%	72	28,8%	386	35,3%
Mayor capacitación para usuarios	233	27,7%	61	24,4%	294	26,9%
Precios más accesibles	222	26,4%	62	24,8%	284	26,0%
Incorporar estándares internacionales	175	20,8%	95	38,0%	270	24,7%
Mayor facilidad de uso de hardware y software	217	25,8%	52	20,8%	269	24,6%
Honestidad con los usuarios	209	24,8%	40	16,0%	249	22,8%
Productos integrados, que sean seguros de origen	157	18,6%	68	27,2%	225	20,6%
Mayor capacidad técnica y conocimientos	156	18,5%	68	27,2%	224	20,5%
Mejor soporte técnico	142	16,9%	25	10,0%	167	15,3%
Mejores condiciones comerciales	117	13,9%	37	14,8%	154	14,1%
Mayor difusión / divulgación	111	13,2%	28	11,2%	139	12,7%
Más involucramiento con las necesidades del cliente	95	11,3%	32	12,8%	127	11,6%
Mejoras en sus productos	99	11,8%	14	5,6%	113	10,3%
Sistemas compatibles / Integración multimarcas	68	8,1%	40	16,0%	108	9,9%
Soluciones ad-hoc para cada empresa	76	9,0%	29	11,6%	105	9,6%
Información más comprensible	76	9,0%	17	6,8%	93	8,5%
Dar más Información de soluciones para PyME	59	7,0%	10	4,0%	69	6,3%

De acuerdo a la percepción de los Informáticos, la principal exigencia hacia los proveedores de tecnología, es la incorporación de estándares internacionales a sus servicios o productos (38.0% de los entrevistados de este grupo). Con un nivel menor de menciones, pero con bastante peso aún, los Informáticos demandan una mayor asesoría / consultoría por parte de los proveedores, así como productos integrados que de origen ya incorporen mecanismos de seguridad y una mayor capacidad y conocimientos técnicos por parte de los consultores o personal de ventas de las empresas proveedoras.

GRÁFICA 9



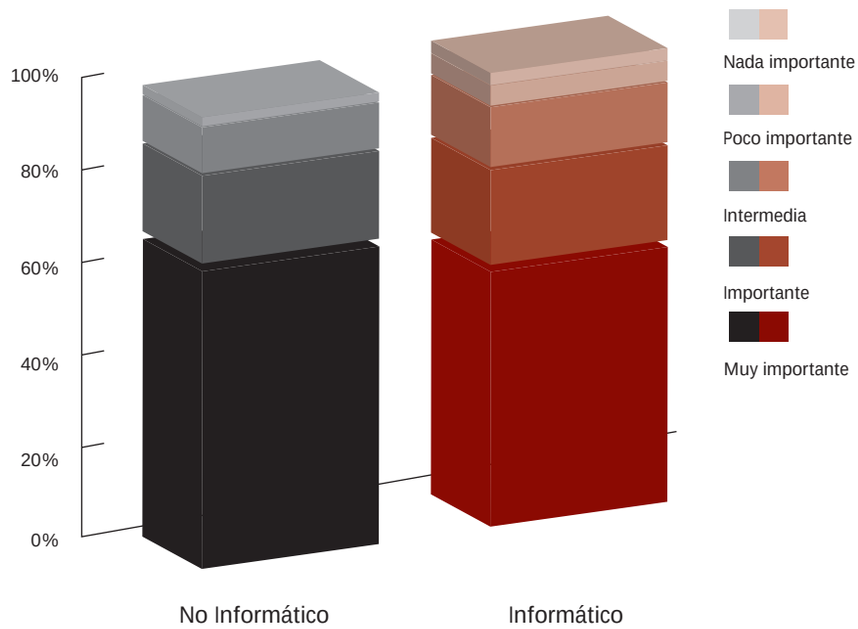
Por su parte, los usuarios No-Informáticos demandan de los proveedores de tecnología una mayor asesoría / consultoría, en primer lugar, seguida de una mayor capacitación por parte del proveedor hacia ellos, precios más accesibles, soluciones de hardware y software que sean más fáciles de usar y honestidad con los usuarios en cuanto a sus recomendaciones, principalmente.

Importancia de la Seguridad en Informática en las empresas

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

La representación de las respuestas a esta pregunta se presenta en la Gráfica 10.

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
Muy importante	571	67,8%	145	58,0%	716	65,6%
Importante	163	19,4%	53	21,2%	216	19,8%
Intermedia	85	10,1%	34	13,6%	119	10,9%
Poco Importante	22	2,6%	13	5,2%	35	3,2%
Nada Importante	1	0,1%	5	2,0%	6	0,5%



GRÁFICA 10

La percepción general de los usuarios (más del 80%), apunta a reconocer que los directivos de su organización sí se preocupan por la Seguridad de la Información.

En general, la mayoría de los entrevistados, tanto No-Informáticos como Informáticos, tienen una percepción positiva acerca de las organizaciones donde laboran, respecto a la importancia que sus directivos dan a la Seguridad de la Información.

Del grupo de los usuarios No-Informáticos, 87.2% opina que la Seguridad de la Información tiene una importancia marcada para sus organizaciones (67.8% Muy importante y 19.4% Importante), mientras que un 79.2% de los Informáticos, aunque en diferente proporción, tiene esta misma percepción (58.0% Muy importante y 21.2% importante). Para el primer grupo, sólo 2.7% de los entrevistados considera que la Seguridad de la información es poco importante o nada importante dentro de las organizaciones donde laboran, mientras que para los Informáticos esta cifra es significativamente mayor (7.2%).

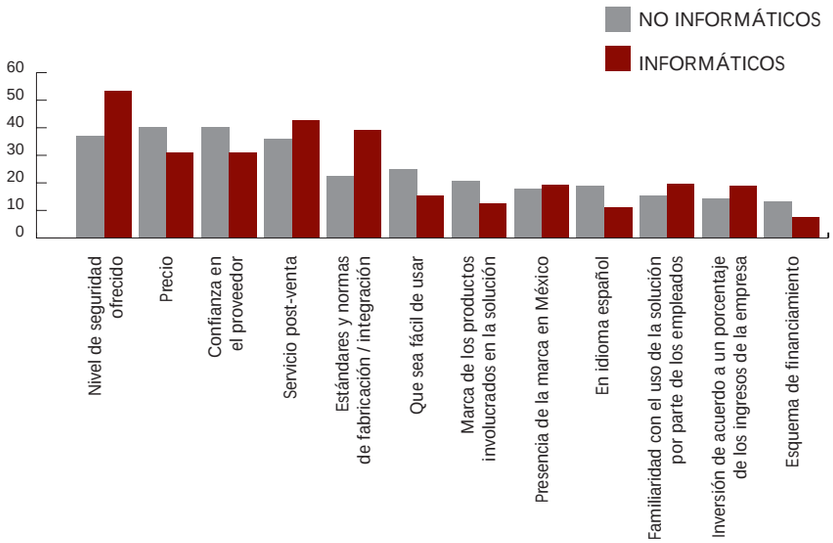
Aspectos a tomar en cuenta en la compra de tecnología

Pregunta: Si usted fuera el responsable de las compras de tecnología de una empresa, ¿cuáles de las siguientes opciones tomaría primero en cuenta? Mencione las 3 más importantes:

La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 6 y en la GRÁFICA 11.

TABLA 6

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
Nivel de seguridad ofrecido	310	36,8%	133	53,2%	443	40,6%
Precio	338	40,1%	77	30,8%	415	38,0%
Confianza en el proveedor	336	39,9%	77	30,8%	413	37,8%
Servicio post-venta	302	35,9%	106	42,4%	408	37,4%
Estándares y normas de fabricación / integración	189	22,4%	97	38,8%	286	26,2%
Que sea fácil de usar	210	24,9%	38	15,2%	248	22,7%
Marca de los productos involucrados en la solución	175	20,8%	31	12,4%	206	18,9%
Presencia de la marca en México	149	17,7%	48	19,2%	197	18,0%
En idioma español	158	18,8%	28	11,2%	186	17,0%
Familiaridad con el uso de la solución por parte de los empleados	129	15,3%	49	19,6%	178	16,3%
Inversión de acuerdo a un porcentaje de los ingresos de la empresa	119	14,1%	47	18,8%	166	15,2%
Esquema de financiamiento	111	13,2%	19	7,6%	130	11,9%



GRÁFICA 11

Para los usuarios No-informáticos, el factor de mayor peso a considerar en la compra de tecnología, es el Precio (40.1%), seguido muy de cerca por el grado de Confianza en el proveedor (39.9%). Resultan también factores primordiales para este grupo, el Nivel de seguridad ofrecido (36.8%) y el Servicio post-venta (35.9%).

Por su parte, estos dos últimos conceptos, en ese orden, son los 2 factores principales a tomar en cuenta por parte de los usuarios Informáticos (Nivel de seguridad ofrecido, con un 53.2%, y Servicio post-venta con un 42.4%), seguido de otros atributos como Estándares y normas de fabricación / integración (38.8%), Precio y Confianza en el proveedor, ambos con un 30.8% de menciones.

Percepción acerca de diversas marcas asociadas con Seguridad en Informática

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

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

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

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

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

TABLA 7

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
NORTON / SYMANTEC	153	18,2%	78	31,2%	231	21,2%
HP / COMPAQ / ATALLA	117	13,9%	37	14,8%	154	14,1%
CISCO	27	3,2%	64	25,6%	91	8,3%
DELL	76	9,0%	13	5,2%	89	8,2%
MCAFEE	55	6,5%	31	12,4%	86	7,9%
KARSPERSKY	55	6,5%	30	12,0%	85	7,8%
APPLE / MAC	57	6,8%	14	5,6%	71	6,5%
ESET / NOD32	49	5,8%	16	6,4%	65	6,0%
IBM / LENOVO	38	4,5%	17	6,8%	55	5,0%
MICROSOFT	39	4,6%	14	5,6%	53	4,9%
SONY / VAIO	45	5,3%	5	2,0%	50	4,6%
PANDA	32	3,8%	8	3,2%	40	3,7%
TOSHIBA	34	4,0%	0	0,0%		3,1%
AVG	12	1,4%	19	7,6%	31	2,8%
CHECKPOINT	5	0,6%	22	8,8%	27	2,5%
AVAST	6	0,7%	20	8,0%	26	2,4%
3COM	8	1,0%	17	6,8%	25	2,3%
SUN / SOLARIS	13	1,5%	12	4,8%	25	2,3%
JUNIPER	3	0,4%	11	4,4%	14	1,3%
UNIX	8	1,0%	6	2,4%	14	1,3%
AVIRA	13	1,5%	-	0,0%	13	1,2%
ACER	11	1,3%	1	0,4%	12	1,1%
TREND MICRO	6	0,7%	4	1,6%	10	0,9%
ADOBE	5	0,6%	4	1,6%	9	0,8%
WINDOWS	9	1,1%	-	0,0%	9	0,8%
LINUX	5	0,6%	3	1,2%	8	0,7%
ORACLE	5	0,6%	3	1,2%	8	0,7%
BARRACUDA	4	0,5%	3	1,2%	7	0,6%
LAVASOFT ADAWARE	1	0,1%	6	2,4%	7	0,6%
SPYBOT	2	0,2%	5	2,0%	7	0,6%
LINKSYS	3	0,4%	3	1,2%	6	0,5%
WEBSENSE	2	0,2%	4	1,6%	6	0,5%
ZONE ALARM	3	0,4%	3	1,2%	6	0,5%
BLUE COAT	2	0,2%	3	1,2%	5	0,5%
INTEL	3	0,4%	2	0,8%	5	0,5%

NINGUNA	4	0,5%	1	0,4%	5	0,5%
REDHAT	4	0,5%	1	0,4%	5	0,5%
MANDRIVA	-	0,0%	4	1,6%	4	0,4%
RSA	1	0,1%	3	1,2%	4	0,4%
SUSE	-	0,0%	4	1,6%	4	0,4%
WATCHGUARD	3	0,4%	1	0,4%	4	0,4%
BITDEFENDER	2	0,2%	1	0,4%	3	0,3%
BMC	1	0,1%	2	0,8%	3	0,3%
FORTINET	2	0,2%	1	0,4%	3	0,3%
HONEYWELL	3	0,4%	-	0,0%	3	0,3%
NESSUS	1	0,1%	2	0,8%	3	0,3%
PGP	1	0,1%	2	0,8%	3	0,3%
SAMSUNG	1	0,1%	2	0,8%	3	0,3%
SOURCEFIRE	-	0,0%	3	1,2%	3	0,3%
SYBASE	-	0,0%	3	1,2%	3	0,3%
TIPPING POINT	-	0,0%	3	1,2%	3	0,3%
Otras	51	6,1%	75	30,0%	126	11,5%
NS/NC	370	43,9%	62	24,8%	432	39,6%

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

TABLA 8

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
NORTON / SYMANTEC	90	10,7%	32	12,8%	122	11,2%
MICROSOFT	40	4,8%	33	13,2%	73	6,7%
PANDA	44	5,2%	22	8,8%	66	6,0%
HP / COMPAQ / ATALLA	49	5,8%	5	2,0%	54	4,9%
MCAFEE	33	3,9%	20	8,0%	53	4,9%
DELL	45	5,3%	7	2,8%	52	4,8%
ESET / NOD	32	3,6%	5	2,0%	35	3,2%
ACER	24	2,9%	10	4,0%	34	3,1%
AVG	22	2,6%	2	0,8%	24	2,2%
WINDOWS	20	2,4%	3	1,2%	23	2,1%
TOSHIBA	17	2,0%	5	2,0%	22	2,0%
IBM / LENOVO	15	1,8%	4	1,6%	19	1,7%
KARSPERSKY	12	1,4%	1	0,4%	13	1,2%
LANIX	10	1,2%	2	0,8%	12	1,1%
APPLE / MAC	6	0,7%	3	1,2%	9	0,8%
NINGUNA	5	0,6%	3	1,2%	8	0,7%
SONY / VAIO	8	1,0%	-	0,0%	8	0,7%
GRATUITOS DE INTERNET	7	0,8%	-	0,0%	7	0,6%
GENERICOS / ENSAMBLADOS	4	0,5%	2	0,8%	6	0,5%
CISCO	2	0,2%	3	1,2%	5	0,5%
TODAS / CASI TODAS	3	0,4%	2	0,8%	5	0,5%
TREND MICRO	1	0,1%	4	1,6%	5	0,5%
BENQ	3	0,4%	1	0,4%	4	0,4%
CA	-	0,0%	4	1,6%	4	0,4%
CHECKPOINT	2	0,2%	2	0,8%	4	0,4%
HAURI	1	0,1%	3	1,2%	4	0,4%
AMD	3	0,4%	-	0,0%	3	0,3%
DLINK	3	0,4%	-	0,0%	3	0,3%
SW	3	0,4%	-	0,0%	3	0,3%
Otras	33	3,9%	23	9,2%	56	5,1%
NS/NC	493	58,6%	124	49,6%	617	56,5%

Qué más les gustaría conocer acerca de Seguridad en Informática

Pregunta: De las siguientes opciones, por favor seleccione los 3 temas sobre los cuales quisiera usted ampliar sus conocimientos.

Ver tabla de frecuencias de la muestra total (Tabla 9) y el comparativo entre Informáticos y No-Informáticos, ordenado por importancia para cada grupo (Tabla 10).

TABLA 9

	No-Informático		Informático		Total	
	x= 842		x= 250		x= 1,092	
Seguridad en Informática en general / todo	234	27,8%	65	26,0%	299	27,4%
Avances y tendencias tecnológicas	217	25,8%	55	22,0%	272	24,9%
Virus	203	24,1%	15	6,0%	218	20,0%
Hackers	136	16,2%	41	16,4%	177	16,2%
Seguridad en Internet	132	15,7%	33	13,2%	165	15,1%
Phishing / Engaños intencionales	113	13,4%	48	19,2%	161	14,7%
Seguridad en Comercio Electrónico	120	14,3%	34	13,6%	154	14,1%
Monitoreo y administración de redes	87	10,3%	57	22,8%	144	13,2%
Spyware / Adware	125	14,8%	16	6,4%	141	12,9%
Control de acceso / Identidad	101	12,0%	29	11,6%	130	11,9%
Encripción de datos / cifrado / encapsulado	83	9,9%	45	18,0%	128	11,7%
Información sobre las empresas de seguridad en informática	85	10,1%	42	16,8%	127	11,6%
Recuperación de datos en general	101	12,0%	26	10,4%	127	11,6%
Seguridad en informática personal / en el hogar	104	12,4%	21	8,4%	125	11,4%
Planes de Recuperación ante Desastres	72	8,6%	51	20,4%	123	11,3%
Hardware y software de seguridad	97	11,5%	18	7,2%	115	10,5%
Información sobre riesgos	84	10,0%	26	10,4%	110	10,1%
Más acerca de agresores internos	79	9,4%	17	6,8%	96	8,8%
Seguridad en telecomunicaciones	74	8,8%	19	7,6%	93	8,5%
Políticas y procedimientos / Mejores Prácticas a nivel mundial	44	5,2%	39	15,6%	83	7,6%
Combate contra Spam (correo no deseado)	71	8,4%	9	3,6%	80	7,3%
Costo-Beneficio de los diferentes productos y servicios ofertados	62	7,4%	18	7,2%	80	7,3%
Tecnología inalámbrica	62	7,4%	14	5,6%	76	7,0%
Regulación / Normatividad / Legislación	40	4,8%	12	4,8%	52	4,8%

Las menciones de mayor frecuencia en ambos grupos de entrevistados, giraron alrededor de aspectos generales sobre el tema (sin especificar).

Entre los temas de mayor interés para los No-Informáticos, en orden de importancia, están los Avances y tendencias tecnológicas sobre seguridad de la información, prevención contra Virus y prevención contra Hackers, principalmente.

Por su parte, los temas de mayor interés manifestados por el grupo de Informáticos, fueron Monitoreo y administración de redes, Avances y tendencias tecnológicas sobre el tema, Planes de Recuperación ante Desastres (DRP), Phishing y engaños intencionales y encripción y cifrado de datos, principalmente.

Principales diferencias entre No-Informáticos e Informáticos

A continuación se enlistan las respuestas de ambos grupos de entrevistados, respecto de los temas sobre los que quisieran conocer más.

TABLA 10

	No-Informático	Informático
1	Seguridad en Informática en general	Seguridad en Informática en general
2	Avances y tendencias tecnológicas	Monitoreo y administración de redes
3	Virus	Avances y tendencias tecnológicas
4	Hackers	Planes de Recuperación ante Desastres
5	Seguridad en Internet	Phishing / Engaños intencionales
6	Seguridad informática personal / hogar	Encripción de datos
7	Seguridad en Comercio Electrónico	Información sobre las empresas de S.I.
8	Spyware / Adware	Hackers
9	Información sobre las empresas de S.I.	Políticas / Mejores Prácticas en el mundo
10	Control de acceso / Identidad	Seguridad en Comercio Electrónico
11	Monitoreo y administración de redes	Seguridad en Internet
12	Encripción de datos	Control de acceso / Identidad
13	Phishing / Engaños intencionales	Recuperación de datos en general
14	Hardware y software de seguridad	Información sobre riesgos
15	Más acerca de agresores internos	Seguridad informática personal / hogar
16	Recuperación de datos en general	Seguridad en telecomunicaciones
17	Seguridad en telecomunicaciones	Hardware y software de seguridad
18	Planes de Recuperación ante Desastres	Costo-Beneficio de productos y servicios
19	Información sobre riesgos	Más acerca de agresores internos
20	Costo-Beneficio de productos y servicios	Spyware / Adware
21	Tecnología inalámbrica	Virus
22	Políticas / Mejores Prácticas en el mundo	Tecnología inalámbrica
23	Combate contra Spam	Regulación / Normatividad / Legislación
24	Regulación / Normatividad / Legislación	Combate contra Spam

Resulta interesante observar que entre las primeras ocho menciones de ambos grupos, coinciden sólo 3 conceptos: Seguridad en Informática en general, Avances y tendencias tecnológicas y Hackers, aunque mencionados algunos de ellos con una prioridad distinta.

Otro hallazgo a notar, es que Políticas y Mejores Prácticas ocupa la posición 9 en el interés de los Informáticos y es la número 22 entre los No-Informáticos.

Spam y cuestiones relacionadas con la Regulación, Normartividad y Legislación, fueron los temas menos mencionados de ambos grupos.

III. ESTUDIO CON EXPERTOS Y PROVEEDORES LÍDERES DEL MERCADO TI

OBJETIVOS DEL ESTUDIO

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

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

METODOLOGÍA

Método de investigación

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

Relación de entrevistados

Empresa	Nombre	Puesto
AXA Seguros México	Luis Expedito Corredor Torres	Business information Risk Manager
Citigroup / Banamex	Erika Mata Sánchez	Audit Manager
Citigroup / Banamex	Ricardo Rodolfo Granados Hernández	Audit Manager
Consultor independiente	Gustavo Servín Juárez	Consultor
GITS (I-Netcertus de México)	Raúl Zamora Araujo	Director de Consultoría
Hypersec Latinoamericana	Luis Fernando Guadarrama Romero	Consultor y Analista de Seguridad
Informática El Corte Inglés	Domingo Salgado	Director Técnico
Instituto de Salud del Estado de México (ISEM)	Norma Macedo Flores	Jefe de Unidad de TI
KIO Networks	Srikan Emmanuel Ruiz Mora	Gerente de Seguridad Informática
NA	El entrevistado solicito permanecer anónimo	NA
NA	El entrevistado solicito permanecer anónimo	NA
Nextel de México	Heriberto Trejo Chavarría	Coordinador de Seguridad de TI
Price Waterhouse Coopers	Sandro Ramírez Cruz	Consultor de TI
Salles Sainz - Grant Thornton, S.C	Manuel A. Llano Sánchez	Gerente de Auditoría de TI
Scitum	Héctor Acevedo Juárez	Product Manager - SOC
Scitum	Jorge Rodríguez Salazar	Director de Servicios Administrativos
Seguros Monterrey New York Life	José Martín Gómez Hernández	Coordinador Auditoría de TI
Sky	José G. Morales Morales	Information Security Manager

RESULTADOS

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

Para efectos clasificatorios, el entorno internacional inmediato y predominante de México podría dividirse en 2 principales grupos: Por un lado, el llamado primer mundo o países desarrollados, delimitado por Estados Unidos, Canadá y los países de la Unión Europea, principalmente aquéllos ubicados en la región occidental. El otro grupo de países con los que México mantiene interacción frecuente y de negocios, es América Latina.

En este contexto se puede decir, de manera general, que en materia de seguridad de la información México se encuentra en un nivel intermedio, equiparable o incluso superior al de la mayoría de países latinoamericanos, pero en un nivel muy por debajo de los países desarrollados. Sin embargo, hay quien opina que este rezago se da sólo a nivel de ejecución, puesto que en el ámbito de la comprensión y el conocimiento, nuestro país está en un proceso avanzado de formación, de hecho debe mantenerse al nivel, para responder a las presiones regulatorias a las que están sujetos, por igual, los países más avanzados.

También es conocido el hecho de que la generalidad no aplica a todo el país por igual. Las organizaciones grandes tienen una mayor conciencia respecto del valor de su información, de la responsabilidad que tienen al manejar información de terceros, se esfuerzan más en difundir una cultura sobre el tema al interior de sus organizaciones, cuentan con un presupuesto mayor y mejor estructurado. No así gran parte de las empresas medianas y la mayoría de las pequeñas. Éste ha sido un tema recurrente a través de los diversos años en los que se realizado el estudio, e indica claramente el área de oportunidad que se tiene en las empresas medianas y pequeñas en nuestro país.

Principales rezagos

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

- Una cultura de seguridad poco extendida.
- Falta de capacitación tanto de los responsables de la seguridad de la información a nivel interno, como de algunos proveedores de soluciones relacionadas.
- Falta de una legislación clara y suficiente. Este ha sido un tema en el que a pesar de haber muchas iniciativas, se percibe que el país está lejos de tener una estructura legal que permita hacer frente a los retos que se tienen respecto de la seguridad en informática. El tema se ha repetido en los cinco años en los que se ha llevado a cabo el estudio.
- Bajo nivel de conciencia entre directivos de las organizaciones.
- Carencia de foros y de presupuesto para incentivar la investigación tecnológica.

Principales progresos

- Las grandes empresas, en general, ya se encuentran en los niveles más altos en el ámbito mundial.
- La conciencia sobre el tema está creciendo. Se está empezando a reconocer que la seguridad de la información es un punto clave dentro de las organizaciones.

OBSERVACIONES MÁS RELEVANTES

"El problema no radica en los sistemas de información, sino en la cultura informática de las personas".

"Se puede dividir la respuesta en dos partes. (1) Comparado con el entorno Latinoamericano, en un nivel mejor de entendimiento y reconocimiento del tema, pero en un nivel de ejecución similar o no muy superior. (2) Comparado con el entorno Europa y Norteamérica, en un nivel técnico de entendimiento similar, pero con menores capacidades de ejecución. Sin embargo, por nuestra cercanía física y en materia de negocios, la presión regulatoria nos afecta a la par que a los países más avanzados (por ejemplo, por el tema SOX, o la LOPD), lo cual nos lleva a tener un reto similar o igual que el que enfrenten países más avanzados, con entornos económicos, tecnológicos y culturales más favorables que el nuestro. En conjunto, México tiene una posición desfavorable, con grandes retos por abordar y con menos medios para hacerlo de manera exitosa".

"Se llevan a cabo iniciativas aisladas de personas o grupos que intentan evangelizar a los niveles de decisión en las organizaciones, sin embargo estos últimos, en su mayoría, muestran marcadas ausencias en el conocimiento del tema y son irracionales en su visión de riesgos al negocio".

"No se tiene legislación clara y suficiente respecto de protección de datos personales. La seguridad informática no tiene el suficiente apoyo, porque no es obligación la protección adecuada respecto de confidencialidad".

"No existe una percepción clara sobre la necesidad de la seguridad informática, como una forma de obtener ventajas competitivas".

"Falta mucha concientización sobre las funciones y responsabilidades de las empresas al respecto de contar con un grupo especializado en la atención de los temas de seguridad".

"Son contadas las empresas que cuentan con la figura de un Oficial de Seguridad y de un Comité especializado en la materia".

"Hay empresas y organizaciones muy comprometidas con el tema y con una cultura madura en temas de Seguridad Informática, al igual que en otros países del mundo. Tal es el caso de entidades financieras, algunas empresas del sector transporte, etc."

"Con lo que respecta a Centro y Sudamérica (excepto Brasil), México se encuentra a la vanguardia y con miras a crecimientos importantes en este ramo; la seguridad en México está dejando de ser un lujo, para convertirse en una necesidad".

"Muchas empresas consideran que sus ciclos de negocio no están relacionados con las prácticas de seguridad de información, sin embargo el gran avance de la tecnología debe impulsar la toma de medidas para dar una prioridad alta a la seguridad de información".

"No se asigna el suficiente presupuesto para este fin".

"México se está renuente a adoptar de forma inmediata nuevas tecnologías en seguridad informática, mientras no sean adoptadas de manera general. Esto derivado del rechazo a utilizarlas en el momento que son puestas en el mercado, debido a que se etiquetan como modas".

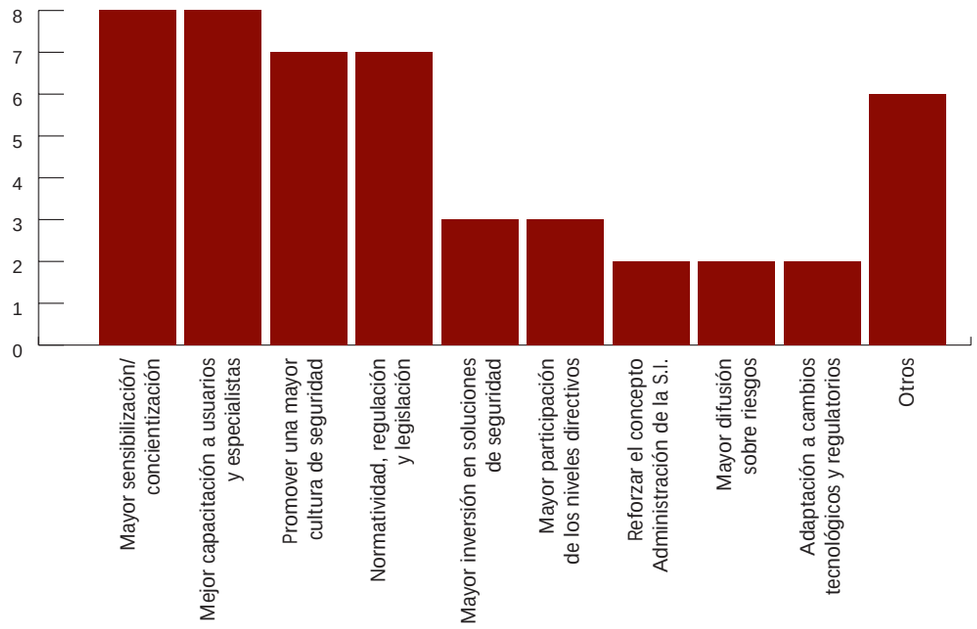
Principales retos de México como país, en materia de Seguridad en Informática

Las respuestas codificadas de todos los entrevistados pueden observarse en la Gráfica 12.

En general se considera que en diversos niveles organizacionales, hace falta conciencia tanto alrededor del valor de la información, como acerca de los mecanismo que existen para protegerla, no sólo hablando de tecnología, sino de otro tipo de recursos como son el análisis de procesos, la difusión de normas y mejores prácticas, etc. Se tiene la percepción de que la alta dirección, en general, aún no tiene conciencia plena de las implicaciones y el impacto que ciertas vulnerabilidades pueden tener en sus propios negocios, por lo que las inversiones en seguridad de la información suelen estar en niveles muy bajos.

La capacitación es otro de los retos más importantes a enfrentar, no sólo en lo que se refiere a promover un mayor conocimiento por parte de los usuarios, sino también de los especialistas del ramo, quienes tienen que adaptarse con rapidez a la dinámica de las reglas a nivel internacional, nacional y local, así como a la nueva tecnología.

GRÁFICA 12



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

- Planes de apoyo a empresas de todos los niveles.
- Promover el intercambio de experiencias entre organizaciones.
- Mayor participación, como industria, en eventos de nivel internacional.
- Evitar la desaparición de empresas pequeñas del ramo.
- Acelerar el nivel de adopción de la tecnología.
- Apoyar más la investigación tecnológica sobre Seguridad de la Información.

OBSERVACIONES MÁS RELEVANTES

"Lograr la concientización en todos los niveles de las organizaciones para que quede claro la importancia y relevancia de atender los asuntos relacionados con seguridad informática (gente, procesos y tecnología), a pesar de la crisis y el recorte de presupuestos".

"Que la gente encargada de la seguridad informática entienda que, al igual que toda área de TI, debe alinearse al negocio y dar valor al mismo, encontrando siempre maneras de hacer más con menos".

"Adoptar realmente los estándares y mejores prácticas de la industria, no por moda o por lograr un certificado, sino como parte de un proceso de mejora continua que agregue valor al negocio".

"Desarrollar un programa de sensibilización efectivo para llevar cultura del tema a las organizaciones y universidades".

"Integrar clusters de proveedores, académicos y empresarios que permitan habilitar equipos de trabajos multidisciplinarios para poner en práctica planes de apoyo a las empresas de todos los niveles".

"Promover sesiones permanentes para compartir experiencias de éxito, derivadas de los planes de apoyo a empresas, escuelas e industria".

"Generar normativas y regulaciones mexicanas, aplicables a las empresas públicas y privadas para obligarlas a implantar mecanismos de protección a la información".

"Crear un entendimiento sobre los beneficios de un gobierno de seguridad de la información".

"Establecer una relación estrecha con la alta gerencia para que la seguridad de información sea una de las partes importantes en el negocio, recibiendo el apoyo y participación activa de este nivel".

"La desaparición de pequeñas empresas dedicadas a la seguridad, como consecuencia de políticas gubernamentales y tendencias que favorecen la asignación de grandes proyectos y contratos a grandes empresas".

"Conocimiento y capacitación sobre herramientas de seguridad, que se incluya al menos una materia básica dentro del plan de estudios de las universidades".

"Legislación acorde a la era de la tecnología. Por ejemplo, un delito no puede perseguirse igual en todos los sentidos cuando se comete por medios tecnológicos, y esto abarca formación y transformación del aparato judicial. Esto no es un tema tecnológico".

"Incorporación, adopción y adaptación de tecnologías no diseñadas o no pensadas para nuestro particular entorno".

Impacto que podría tener la situación económica mundial de 2009 en la percepción sobre Seguridad de la Información por parte de la gente

Según la mayoría de los expertos entrevistados, las inversiones en materia de Seguridad en Informática podrían mantenerse bajas e incluso decrecer, sobre todo en organizaciones medianas y pequeñas. El panorama podría ser difícil, como consecuencia, para los proveedores de la industria, pero lo que es más grave, podría significar un entorno informático más inseguro en general.

Algunos manifestaron el temor de que los empresarios lleguen a percibir que "se puede vivir sin seguridad de la información" o bien que la inversión en este renglón "puede postergarse al largo plazo, ya que no representa una necesidad de atención inmediata". Se percibe que la prioridad de las empresas en general, y de todo tipo de organizaciones, estará enfocada a destinar recursos económicos a otros rubros, como el sostenimiento del empleo, el abastecimiento de materias primas y de suministros vitales, el pago de servicios, pago de impuestos, etc.

Se estima que "Directores y comités de las empresas, estarán dispuestos a absorber mayores riesgos para no tener que invertir en seguridad, a menos que ésta sea renovada por carácter obligatorio, por ejemplo por la Comisión Nacional Bancaria y de Valores hacia las instituciones financieras".

En contraparte, existen algunas opiniones optimistas respecto de que este fenómeno representa una buena oportunidad para demostrar que la Seguridad de la Información es primordial dentro de una organización.

Un punto de vista interesante, puede apreciarse en la siguiente cita:

"Generalmente cuando hay crisis o recesiones, disminuyen las ofertas de trabajo y se reducen las plantillas de las organizaciones. El tema de despidos es una amenaza latente que puede causar daños a las organizaciones. La gente tendría resentimientos o motivos para querer dañar a la organización, por despido o en colusión con la gente que se queda".

"Por otro lado, la percepción respecto a la Seguridad de la Información en tiempos de crisis podría verse como un estancamiento en ciertos temas o como disminución en los controles, dados los recortes presupuestales".

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

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

- La optimización de los recursos económicos: cómo hacer más con menos.
- La sensibilización de sus empleados y la formación de una cultura organizacional de participación colectiva cuando se implanten políticas y procedimientos de control a la seguridad.
- Claridad y una buena difusión en cuanto a la normatividad interna.
- Justificación del costo de inversión en infraestructura.
- Certidumbre en cuanto a que su información está siendo tratada con la debida diligencia, y que los servicios requeridos cuentan con los controles necesarios para garantizar seguridad de transacciones e intercambio de información.

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

Entre los retos más mencionados, están las siguientes:

- Proporcionar soluciones más integrales.
- Tener la capacidad para formalizar y cumplir Niveles de Servicio.
- Mantener su competitividad, a través de innovación continua y acciones de valor agregado.
- Proporcionar seguridad a la medida de la problemática específica y necesidades de los clientes.
- Proveer de un verdadero apoyo a las empresas con un enfoque de negocio y no solamente técnico. Comprender que las herramientas son un componente de apoyo para las soluciones integrales, no lo son todo.
- Actualización tecnológica y de conocimientos permanente.
- Entregar ofertas de valor que incluyan implantación optima del hardware y software.
- Atención oportuna y solución a los problemas o incidentes que se pudiesen presentar.
- Proveer un buen nivel de capacitación a los responsables finales del hardware y software.
- Capacidad de garantizar y brindar elementos para una mayor velocidad en la adopción tecnológica.

OBSERVACIONES MÁS RELEVANTES
"En tiempos de crisis el reto mas importante es la competitividad y la honestidad con los clientes respecto al alcance, beneficios y oportunidades de los productos que venden"
"Alinearse a servicios de seguridad, no sólo a la venta de 'cajas'. Deben proporcionar un servicio completo".

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

De manera general, se percibe que los programas educativos a nivel universitario, aún adolecen de una falta de contenidos enfocados a fortalecer una cultura de Seguridad de la Información entre los alumnos de distintas carreras. Una de las principales coincidencias entre los expertos entrevistados, es que las instituciones educativas deben dar un mayor énfasis en el desarrollo de estrategias de enseñanza como parte integral de los programas académicos, planteando problemáticas reales e incentivando a los alumnos a crear propuestas específicas que aporten nuevas opciones de solución. No se trata únicamente de hacerlo en las carreras relacionadas con tecnología, sino en todas las especialidades, ya que la seguridad de la información no es exclusiva de las ingenierías y la informática, sino de toda la sociedad en su conjunto.

En otro contexto se mencionó que uno de los retos más importantes a enfrentar, no sólo por parte de las instituciones educativas sino del sistema y el Estado en general, es el de atraer estudiantes sin poder asegurarles empleo al final de sus estudios. Esto está relacionado con la falta de Investigación Formal en el país, lo cual sería una fuente de empleo y de desarrollo para México.

Otros temas de interés giraron alrededor de las asignaciones presupuestales a la investigación tecnológica y el desarrollo de herramientas o mecanismos de apoyo a la seguridad de la información, en contextos específicos de nuestro país y sus diversas industrias.

OBSERVACIONES MÁS RELEVANTES
"Desarrollar un plan de educación en donde se tengan contemplados temas relacionados a la seguridad de información, sin importar distinción de carrera, ya que al final todos participaran por un mismo objetivo que es el buen funcionamiento de la organización como equipo de trabajo".
"Preparar a los estudiantes en temas de seguridad informática, así como, crear especialidades que generen profesionales para la investigación de nuevos y/o mejores mecanismos de seguridad".
"Capacitación adecuada en procesos y recursos humanos, con enfoque de la seguridad informática".
"Enseñar a pensar, más que dar conocimientos".
"Facilitar el uso de sus instalaciones en pro de la capacitación en materia de Seguridad de la Información".

JFS KIO Networks Secure Information Technologies Universidad Iberoamericana Ciudad de México

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

Los medios de comunicación en general, tienen una responsabilidad de mucho peso en el manejo de este tema, dado que los riesgos pueden alcanzar cada vez a más personas, como consecuencia de la gran interacción que se da entre los cada vez más usuarios de Internet. Los medios tienen la capacidad de llegar a todos los ámbitos y difundir contenidos de prevención tanto en el ámbito organizacional (con temas como redes, servicios administrados, políticas y procedimientos, mejores prácticas, normatividad, etc.), personal (a través de la difusión de riesgos y consejos para usuarios de las redes sociales, por ejemplo) y aspectos que tocan por igual a ambos grupos, como el uso del correo electrónico, el manejo de identidad, la utilización de banca por Internet, comercio electrónico, cuidado de los equipos e infraestructura, etc.

Un gran número de opiniones giraron alrededor del sensacionalismo o amarillismo que suelen explotar los medios, sin una estrategia clara de educación o concientización. Suelen destacar lo que les ayuda a vender sus medios o sus tiempos, sin una dialéctica planeada que permita a la audiencia cerrar los conceptos con recomendaciones y soluciones para evitar caer en situaciones similares. Es notorio destacar que en los cinco años en los que se ha realizado este estudio, no parece haber mejoría en la percepción del papel que juegan los medios.

Los mismos medios de comunicación tienen una responsabilidad en cuanto a la integridad y confidencialidad de las personas u organizaciones, sobre las que manejan información. Uno de los retos en este sentido, es la sensibilización y capacitación del personal que tiene a su cargo la comunicación de las noticias y del contenido editorial.

OBSERVACIONES MÁS RELEVANTES
“Generar campañas publicitarias inteligentes, sin competencia con otros medios, uniendo esfuerzos en pro del bienestar nacional, de la formación educativa, de la preservación de las empresas e industria”.
“Presentar o reportar los casos de incidencias de seguridad, no para crear pánico o con fines amarillistas, sino para crear conciencia de que las amenazas existen y que estamos propensos”.
“Deben enfocarse a decir las cosas, pero también a decir el cómo se pueden prevenir o qué es lo que se está haciendo al respecto. Por ejemplo el caso clásico de robo de identidades en las tarjetas bancarias, sólo mencionan el cómo se hizo, sin embargo no dan a conocer los mecanismos de seguridad por los cuales estos actos pueden ser prevenidos”.
“Ellos mismos requieren concientización, entendimiento y un código de ética estricto que refuerce la protección de las organizaciones o individuos de los que divulgan información”.
“Actualización de conocimientos sobre todo en las personas encargadas de difundir noticias y opiniones de manera masiva”.
“Promoción de artículos relevantes de interés general en aspectos de riesgos y seguridad por parte de especialistas en la materia, considerando su afectación económica y su repercusión para una Organización”.
“Destacar las campañas que se llevan a cabo en países del primer mundo con respecto a la seguridad; esto deberá de ser dirigido a CIO´s”.

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

Se consideran prioritarios al menos dos aspectos en donde el gobierno debería poner énfasis. Por un lado, está la creación de leyes claras que permitan regular las actividades relacionadas con la confidencialidad de la información, los delitos informáticos, el establecimiento de reglas claras para las telecomunicaciones y otros ámbitos que den certidumbre tanto a los inversionistas del ramo como a la sociedad en general. Por otro lado, es precisa una mayor intervención de los diferentes órganos de gobierno en la difusión de la seguridad de la información, tanto a nivel interno entre funcionarios, niveles intermedios y usuarios de la información gubernamental y de la ciudadanía, como hacia el exterior.

Asimismo, se menciona que el gobierno debe tomar la responsabilidad como coordinador de los esfuerzos de diferentes instituciones y organizaciones, para establecer programas de acción y difusión sobre el tema.

Entre otros de los principales retos mencionados, también destacaron:

- La recuperación de la credibilidad y la confianza, en esta materia.
- La formación de una cultura de seguridad que permita diseminar una mayor conciencia y conocimiento.
- La iniciativa de protección de datos personales.
- La modernización de esquemas de recolección de impuestos
- La certificación de procesos de desarrollo de software
- La apertura en los diferentes ámbitos de la seguridad informática
- La comunicación e intercambio de conocimientos con otras naciones, organizaciones y asociaciones.

OBSERVACIONES MÁS RELEVANTES
"Liderar los programas de vinculación con todos los grupos mencionados anteriormente, buscando cooperación de especialistas y asociaciones sin fines de lucro, que aporten valor real y expedito a dichos programas".
"Generar instituciones de vigilancia que se encarguen de auditar el cumplimiento a regulaciones, sobre todo las que tengan que ver con la protección de información de los ciudadanos".
"Integración de servicios, buscar economías entre aéreas".
"Exigencia en la aplicación de normas y mejores prácticas de Seguridad, tal como la ISO27001, así como la disposición de recursos adecuados y personal certificado para la práctica y vigilancia en la gestión de la Seguridad de la Información".
"Promover legislaciones y reglamentos adecuados para normar y conducir las TI en un medio seguro y predecible".
"Educar a las entidades regulatorias y al aparato jurídico en estos aspectos".
"Congruencia y Definición. Cambios radicales. El Gobierno se percibe como la mayor fuente de inseguridad".

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

AXA Seguros México | **Luis Expedito Corredor Torres** |*Business Information Risk Manager*

"Compromisos éticos con nuestros clientes en materia de protección de datos, siguiendo estándares, lineamientos y legislaciones aceptadas internacionalmente".

Citigroup /Banamex | **Erika Mata Sánchez** | *Audit Manager*

"Dos importantes que vienen a la mente: el tema de concientización y formación a todos los colaboradores de la organización, y la innovación en esquemas de control de acceso y protección de transacciones financieras a través de medios electrónicos".

Citigroup /Banamex | **Ricardo Rodolfo Granados Hernández** | *Audit Manager*

"Citi ha sido siempre modelo a seguir en la implementación de medidas de seguridad de la información. La metodología para realizar las auditorias en esta materia, tiene reconocimiento a nivel mundial".

GITS (I-Netcertus de México) | **Raúl Zamora Araujo** | Director de Consultaría

"Implementar tecnología de vanguardia para garantizar operaciones electrónicas, principalmente de los sectores financiero, retail, industria y servicios latinoamericanos".

Hypersec Latinoamericana | **Luis Fernando Guadarrama Romero**
Consultor y Analista de Seguridad

"Desarrollando productos, servicios y capacitación en seguridad y "software testing", para empresas dedicadas al desarrollo de software".

KIO Networks | **Srikan Emmanuel Ruiz Mora** | Gerente de Seguridad Informática

"Estamos por iniciar el proceso de certificación del SOC en ISO 27001. Esta certificación tiene como primer objetivo el auditar todas las normas, procedimientos y controles con las que al día de hoy cuenta el SOC de KIO Networks, y validar que éstos se acoplan a las mejores prácticas y estándares de la industria.

Para KIO, el obtener esta certificación es de gran importancia, ya que es la forma de demostrar a nuestros clientes que su información está segura con nosotros, dándoles con esto la tranquilidad que se merecen.".

Nextel de México | **Heriberto Trejo Chavarria** | Coordinador de Seguridad IT

"La formación de un grupo de seguridad y el desarrollo de su nivel de madurez, que atiende los rubros sobre monitoreo de seguridad, control de accesos y cumplimiento regulatorio".

PriceWaterhouseCoopers | **Sandro Ramirez Cruz**
Consultor de tecnologías de la información

"Las aportaciones principales de la organización, son iniciativas para lograr el manejo adecuado de la información, referidas a las buenas prácticas, enfocándolas a puntos de calidad como la obtención de certificaciones ISO. Con este tipo de iniciativas, México puede reflejar ante el mundo que cuenta con un nivel aceptable de conocimientos sobre seguridad, tal y como ocurre en países como Japón e India".

Salles Sainz – Grant Thornton | **Manuel A. Llano Sánchez** | Gerente de auditoría de TI

"Apoyando la promoción y difusión de las políticas de seguridad, así como un monitoreo constante de las mismas".

Scitum | **Héctor Acevedo Juárez** | *Product Manager – SOC*

- "Desarrollo de metodologías de operación para cuestiones relacionadas con seguridad informática.
- Difusión de conocimientos de seguridad informática".

Seguros Monterrey New York Life | **José Martín Gómez Hernández**
Coordinador auditoría de TI

"Hace como dos años se estableció una función más formal referente a la seguridad de la información, así como el proyecto de clasificación de la información (aunque esté todavía en una etapa incipiente)".

Sky | **José G. Morales Morales** | Information Security Manager

"Además de estar protegiendo los activos de información de la empresa, se está haciendo énfasis en la concientización del personal en temas de seguridad informática que puedan ser aplicados de manera interna a la organización, pero también de manera personal en su hogar o en cualquier otro lugar (cibercafés, computadoras que no sean de su propiedad y que por alguna razón necesiten utilizar, etc.)".

Por su parte, los entrevistados que prefirieron permanecer anónimos y que sin embargo también brindaron opiniones valiosas y de interés para el presente estudio, mencionaron que sus organizaciones, entre otras aportaciones, han realizado las siguientes:

- "La concientización a los usuarios de nuestros servicios en línea, los está orientando a usar de manera más segura la TI, que hoy está al alcance de casi toda la población con un nivel promedio de escolaridad.

- "El establecimiento de prácticas de primer nivel en la administración de la seguridad informática.

- "La creación de normas, políticas y estándares, que pueden ser de uso general y la certificación en procesos de seguridad de la información que pueden servir de ejemplo a otras Instituciones y el despliegue de programas de concientización".

IV. CONCLUSIONES DE LA INVESTIGACIÓN

Avances importantes en 2009

La percepción, en su mayor parte positiva, que tienen tanto los Informáticos como los No-Informáticos respecto de la importancia que se le da a la seguridad de la información en las empresas u organismos donde laboran, se puede interpretar como un avance importante en la materia. Si se considera que la muestra incluye múltiples sectores, empresas de diversos tamaños y una gran diversidad en los puestos ocupados por los entrevistados, se puede concluir que México está teniendo avances importantes en la atención que las empresas de todos tipos están dando al tema de la seguridad de la información.

Una solicitud que llama la atención, es la que hacen los No-Informáticos hacia los proveedores de tecnología, en el sentido de que sean honestos con los usuarios. Año con año los Estudios de Percepción en Informática en México, han detectado un creciente aumento en la importancia que tiene el tema para los usuarios; esta petición podría significar un aviso de que algunas personas tienen la idea de que hay proveedores que están aprovechando esta inquietud de los usuarios para venderles productos innecesarios o defectuosos.

Comienza a percibirse y comunicarse, entre los expertos en el tema, la importancia de que la Seguridad de la Información debe ser parte de la formación académica en todos los niveles, no sólo de educación computacional o tecnológica. Así como la tecnología informática se está incorporando cada vez más a la vida cotidiana de todas las personas, la seguridad de la información comienza a ser percibida como algo que forma parte intrínseca de la vida actual en México.

Una de las principales preocupaciones de los expertos, es el rezago que existe alrededor de la Regulación, Normatividad y Legislación en México, en materia de Seguridad de la Información. Sin embargo, es de los últimos rubros sobre los cuales los usuarios muestran algún interés.

Aspectos que siguen rezagados

Para los expertos en el tema, sigue habiendo un llamado importante a que mejore la Regulación, Normatividad y Legislación en México, en materia de Seguridad en Informática. Sin embargo, al igual que en años anteriores, estos rubros son de los que menos mencionan los usuarios comunes, tanto Informáticos como No-Informáticos.

Se sigue percibiendo un rezago importante en la creación y aplicación de leyes claras que ayuden a perseguir y castigar los delitos informáticos, lo cual es percibido como una desventaja de México frente a otros países. Además de las claras implicaciones que tiene esto en relación con la problemática que representa para usuarios y la sociedad en general, también ahuyenta la inversión en el país, tanto nacional como internacional.

Se sigue percibiendo que el Gobierno de México debe hacer mayores esfuerzos por promover una cultura de Seguridad de la Información en el país, con énfasis hacia sus propios funcionarios, pero también hacia la sociedad en general.

V. ARTÍCULOS SOBRE SEGURIDAD EN INFORMÁTICA

ALAPSI frente al estudio de percepción de seguridad 2009

Por Raúl Aguirre García
Presidente de ALAPSI 2007-2010

El Problema de Seguridad de la Información en México tiene que ver con los avances en la implementación de un buen sistema de Gestión del Riesgo, lo cual ha tomado su relevancia estos últimos 15 años. A nivel de conciencia, el presente estudio nos dice que hemos avanzado en este esfuerzo y que falta mucho más por el lado de Concienciación en forma integral, en todas las audiencias de nuestras instituciones. Sabemos que hay muchas más empresas que están buscando definir su estrategia de seguridad de la información con un alcance no sólo pequeño o incipiente, con el interés de ir avanzando en la madurez del proceso de administración de riesgos, sin embargo, en la mayoría de los casos, dista mucho aún de contar con un Gobierno de Seguridad efectivo.

Casi todas las empresas financieras, de servicios importantes y grupos corporativos, cuentan con una estrategia de seguridad de información integral, concientes sus altos directivos de que tienen que implementar un sistema de Administración de Riesgos basado en una norma, como por ejemplo ISO27000; sin embargo y sin temor a equivocarme, falta mucho por completar el nivel de madurez adecuado en cada empresa. Por ejemplo, haber pasado ya por lo menos dos ciclos del proceso Deming (instrumentados sus KPI y los KGI, basados en COBIT de ISACA), así como la medición del Gap y el establecimiento del proceso de Mejora Continua. Sin lugar a duda tienen buen avance en las fases de PLAN y DO de Deming, que ven el diseño, las normas de implementación y ejecución de la Seguridad, sin embargo no hay lo suficiente o muy poco en la fase del CHECK que mide con detalle el riesgo residual, de tal manera que conecte con el nuevo ciclo del sistema de Gestión ACT, y de manera iterada se avance en la protección y prevención de la Información apoyados con la revisión de cumplimiento interna y externa.

Por otro lado, como consecuencia del avance de la tecnología, la inseguridad ha aumentado, ya que dichos avances están alcanzando capacidades que facilitan el acceso a todos los niveles o capas de seguridad. De poco más de 1.5 miles de millones de internautas (Revista de Política Digital), y adicionalmente como lo he entendido con la situación de riesgo que se tiene hoy ya en la NUBE de Internet, donde hay servidores y tecnología ocupados a encontrar, identificar, copiar, controlar, analizar tendencias y usos, por parte de grupos coludidos con defraudadores, y utilizar la información para fines económicos, políticos, sociales, negocios sucios, para defraudar y para engañar.

Estoy de acuerdo con Adolfo Grego, quien comentó el porqué del fracaso de la Seguridad, al decir que la falla de los programas de Seguridad se debe a que no hemos sido capaces de explicar, señalar y justificar al comité de Seguridad, cuánto se tiene que gastar, conforme se están implementando las soluciones o los controles, y se puedan medir los resultados para saber cuánto se reduce el nivel de riesgo. No se sabe justificar el gasto o la inversión que se requiere para los proyectos de seguridad, en relación a las necesidades de la institución, ni se sabe informar en cuánto va a reducir el riesgo.

Estamos varados en la problemática de la implementación con el cambio de cultura para tratar

de que los controles sean parte de la operación del día con día. Tenemos que romper el paradigma y continuar con la tercera y cuarta parte del dominio del proceso Deming, y lograr que la Alta Dirección fomente la dinamicidad del ciclo de una manera natural en los procesos y ciclos de su negocio.

¿ALAPSI, como integradora de profesionales, cómo pretende afrontar esta situación de inseguridad?

Lo que tenemos que hacer es seguir avanzando en la conciencia, en la instrucción, en la capacitación y en la práctica de seguridad en las instituciones, desde que se inicia la formación de una conciencia e inquietud profesional, primer paso en la Universidades. Conectar la experiencia con la enseñanza y su formalización universitaria.

Vislumbramos necesario el iniciar con materias de Administración de Riesgos desde la Preparatoria, y con conceptos sencillos y prácticos desde la primaria y secundaria, involucrar a los padres de familia, los maestros, directores de escuela y hasta psicólogos. Hacer sinergias entre profesionales de la educación, las empresas, las instituciones de gobierno, los proveedores de TI.

Es necesario cerrar la pinza del especialista práctico, para que sus resultados se puedan definir en metodologías. Que los especialistas en el campo de trabajo, se apoyen en las universidades para la formalización de sus materias y planes curriculares, el reconocimiento de sus Créditos y la autoridad de su especialidad. Robustecer las certificaciones con avales de su ética y puesta en práctica exitosa.

Invertir en conjunto en la preparación de cursos, talleres, seminarios, diplomados. Ello incluye la preparación de especialistas como instructores, que atiendan esta necesidad.

Desde marzo de 2009, se avanza en la firma de convenios de colaboración con las diferentes universidades.

Hemos iniciado con actividades de motivación y habilitadores de la relación con las universidades a través de las siguientes 5 acciones:

1.- La JORNADA del 14 aniversario de ALAPSI, empezando con dos participantes de cada Comité Universitario.

2.- Continuar con cada Comité Universitario para definir los planes de trabajo y el compromiso de colaboración, todo apegado a su normatividad. Identificar eventos, cursos, talleres, diplomados, seminarios, revisiones de planes y propuestas de estudios de seguridad en diferentes carreras y estudios de posgrado, y apoyar a profesionales en el campo a lograr su certificación y el reconocimiento de sus CPE (Continuing Professional Education credit).

Definir en qué, con quiénes, cómo interactuar y con qué recursos, para concientizar y dar a conocer el Cuerpo de Conocimiento de la Seguridad y su necesidad, así como de las metodologías, técnicas y herramientas para implementarse. Definir cómo será el fomento del Sello ALAPSI, participando especialistas en la revisión de los planes de estudio y propuestas de mejoramiento para la preparación del profesional, tanto en licenciaturas como en posgrado.

3.- Definir entre los Comités Universitarios cómo organizar eventos importantes durante cada periodo. Definir el Premio de Seguridad que fomente su interacción, la formación de un Comité Técnico Especialista, para la generación de las Normas de Evaluación y la definición de los premios, los patrocinadores, el proceso de evaluación y la premiación en el DÍA DE SEGURIDAD o en otro momento dentro de estos 8 meses.

4.- Redefinir cómo integrar a la membresía y su proceso de pertenencia. Lograr implementar un proyecto de tutelaje o de mentoring. A través de la red de comunicación y desarrollo, motivado por reconocimientos, bonos y patrocinios, para su capacitación, su formación, fomentando su avance y especialización, buscando el equilibrio entre el esfuerzo realizado y el tiempo dedicado; fomentar y calificar los valores y la capacidad demostrada en cada especialización como implementador, operador, asesor, consultor, auditor; en sus niveles como Estratega, Táctico u Operador. Este es un esquema a definir e incluso se está proponiendo lanzarlo como uno de los trabajos para el Premio de Seguridad.

5.- Iniciar la preparación del cambio para la nueva Mesa Directiva en el periodo 2010-2013, participando todos los miembros activos. Que la nueva Mesa Directiva cuente con una plataforma de relaciones y oportunidades para interactuar con la Academia y mediar los intereses de las universidades y de los miembros. con la actividad laboral de la ALAPSI. Revisar nuestra normatividad actual para lograr efectividad, participación y desarrollo profesional, que nos está marcando la sociedad en su actividad académica, económica y social, considerando la integración, la consolidación y la trascendencia de la ALAPSI.

Seguridad: El orden de los factores SÍ altera el producto

Por Gilberto Vicente
Security & Mobility Business Development Manager
Cisco Systems de México

No es lo mismo hablar de "tecnología de seguridad" que de "seguridad en la tecnología". Siendo las Tecnologías de Información y Comunicaciones (TIC's) elementos fundamentales de nuestra forma de Vivir, Trabajar y Divertirnos, es fundamental entender cómo éstas pueden convertirse de igual forma en elementos de Protección y Prevención para la Seguridad de nuestra Información.

La reciente epidemia de influenza ocasionada por el virus AH1N1 llevó a la gente a un estado de paranoia, impulsada en gran parte por la influencia mediática y el desconocimiento de la población sobre la verdadera gravedad del problema y los mecanismos adecuados de protección. Pero el paso de los meses y la capacidad de olvido del ser humano originaron una "vacuna mental" que pareciera superar a la misma inmunización física contra el virus, dejando a su paso una capa de negligencia y letargo entre la población. El mismo escenario ocurre en el mundo virtual del que formamos parte personas y organizaciones, donde el grado de exposición es, quizá, mayor, así como también los efectos de la negligencia y la falta de conocimiento y cultura en torno a la importancia de la seguridad de la información.

En estos tiempos, contar con vacunas o paliativos para todas y cada una de las amenazas a las que estamos expuestos es prácticamente imposible, no hay presupuestos que alcancen y seguirá siendo responsabilidad de cada uno de nosotros implementar las medidas de protección necesarias para salvaguardar nuestros activos valiosos. La clave está en la prevención y, focalizándonos en el mundo de Tecnologías de Información, éstas juegan un rol importante como habilitadoras del negocio así como mecanismos de defensa, si son debidamente seleccionadas y utilizadas.

PANORAMA DEL CAMPO DE BATALLA

Desafortunadamente, más allá del sólo hecho de detener ataques, las organizaciones enfrentan distintos retos en materia de seguridad de la información, como lo son:

1. Protección de la información corporativa y los datos personales de clientes y empleados.
2. Garantizar la continuidad e interoperabilidad de los servicios de los que depende el negocio.
3. Generación de conciencia y cultura en toda la organización.
4. Reducción de costos y optimización de recursos operativos.
5. Cumplimento con marcos regulatorios y disposiciones legales.

Por si fuera poco, atender de manera reactiva un escenario de inseguridad ha sido la práctica por excelencia; es decir, las empresas implementan redes y posteriormente instalan firewalls o soluciones de detección y prevención de intrusos para poder protegerlas; implementan servicios de comunicaciones unificadas y erróneamente asumen que "cajas mágicas" pueden ser instaladas posteriormente para proteger toda una arquitectura, etc.

Es esta práctica obsoleta, sin lugar a dudas, una de las principales razones por las que naturalmente los esfuerzos de seguridad se perciben como meramente operativos o centros de costo en las organizaciones.

DESCUBRIENDO EL HILO NEGRO

Afortunadamente, para los retos anteriormente enlistados, existen consideraciones sencillas y un factor común en cada rubro para atender los retos de forma holística:

1.Análisis de Riesgos, Seguridad Integrada a los procesos y a la tecnología para la prevención de fuga de información

2.Análisis de Riesgos y Seguridad Integrada

3.Alineación al Negocio, Campañas de Educación y Seguridad Integrada

4.Seguridad Integrada

5.Seguridad Integrada, Apego a Mejores Prácticas y/o Estándares de Industria

El énfasis que hacemos en la importancia de la Seguridad Integrada en la Tecnología, como parte de una arquitectura o servicio, se debe a que estos planteamientos son una realidad en la oferta de compañías líderes que han tenido la capacidad de evolucionar de acuerdo a la demanda de un mercado cansado de poner parches (cajas puntuales) y luchar por la justificación del caso de negocio de la importancia de la seguridad.

Es fundamental que las personas y organizaciones comiencen a activar todos aquellos servicios de seguridad presentes en su tecnología, que cuestionen a sus proveedores al respecto e, independientemente del planteamiento (Base de Datos, Data Center, Comunicaciones Unificadas, LAN, WAN, Sistema Operativo, etc.), abandonen la idea de que existen soluciones mágicas a todos los problemas de seguridad.

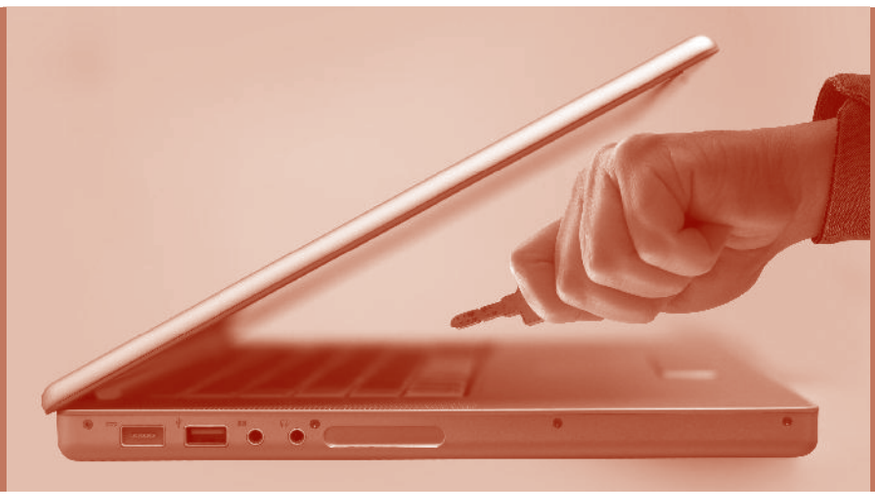
ACTÚE. HOY ES EL MOMENTO

Ciertamente la Tecnología por sí sola no es la solución a todos los problemas de seguridad, y menos aún si se ve como un tema aislado. La fórmula cambia radicalmente cuando tomamos en consideración los procesos y la gente que soporta los objetivos de negocio de la organización, así como cuando demandamos seguridad integrada en cada planteamiento; de ésta forma, la seguridad y las TICs quedan alineadas perfectamente a las prioridades de la organización, convirtiéndose en verdaderos habilitadores de nuevos servicios, reducción de costos y optimización de procesos.

En Cisco Systems tenemos la visión y el compromiso de cambiar la forma bajo la cual las personas viven, trabajan y se divierten. Bajo el entorno que vivimos de Redes sin Fronteras, la seguridad es un factor fundamental en el diseño, construcción y entrega de cada uno de los productos y arquitecturas que presentamos a nuestros clientes, lo que nos ha permitido alcanzar la posición No. 1 a nivel mundial en participación del mercado de seguridad.

Sin importar el tamaño o giro de su organización, lo invitamos a contactarnos y permitirnos ayudarle a responder a sus necesidades de Seguridad de la Información de forma integral.

CISCO SYSTEMS DE MÉXICO
http://www.cisco.com
Cd de México (55) 5267 1000
Monterrey, NL (81) 8221 5050



JFS

El cambiante perfil del "Hacker"

Por Juan Francisco Serrano Kacz
Director General de Joint Future Systems

"Hacker" es el término que se utiliza para referirse a una persona que obtiene acceso a datos electrónicos, mediante el rompimiento de candados electrónicos (claves de usuario por ejemplo).

Hay varias teorías respecto de cómo surge el nombre, pero en general la más aceptada es la de que viene del inglés hack, (que significa darle golpes a algo, hasta que se rompe.)

En un principio, a finales de los 80's y principios de los 90's, los hackers comenzaron a atacar los sistemas de telefonía. Uno de los casos más famosos se documenta en el libro "The Hacker Crackdown" que describe en detalle cómo un hacker pudo, a través de diversas técnicas entre las que se incluyó ingeniería social (obtener información directamente platicando con personas) y el manipuleo electrónico de información, provocar fallas en todo el sistema telefónico de Estados Unidos, re-enrutar números de emergencia para que contestaran en lugares de sexo telefónico, etc. etc.

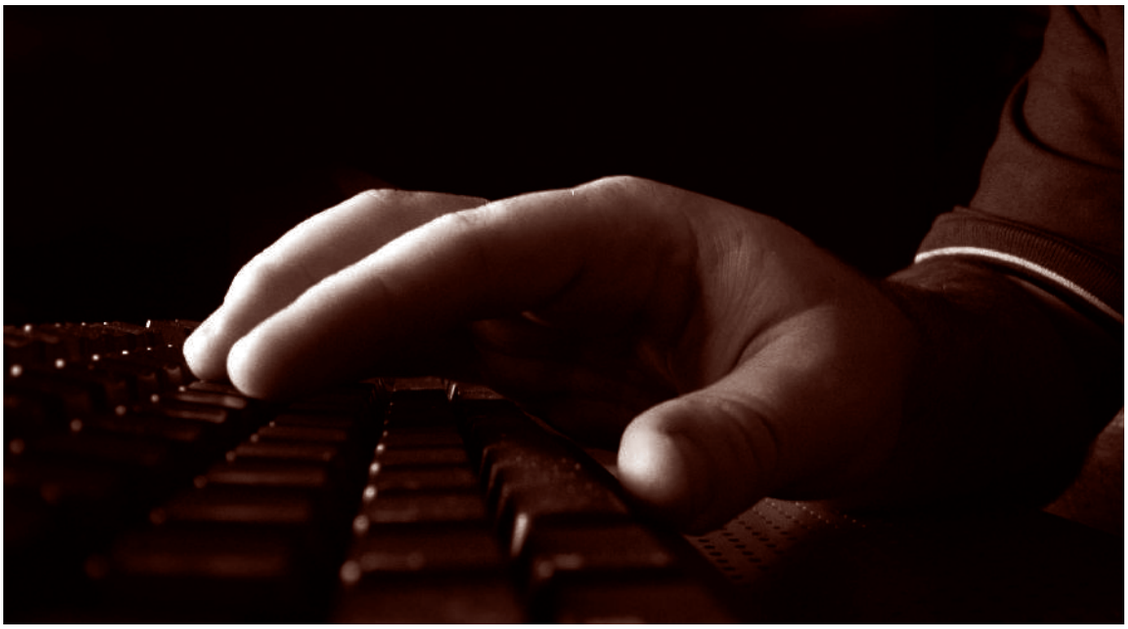
¿Cuál era la motivación para hacer todo esto? Básicamente el reconocimiento de una comunidad de personas conocedoras de tecnología, que usaban nombres en clave y que competían para ver quién era el mejor. Ejemplos de nombres utilizados en aquella época son: Knight Lightning, Leftist, Compu-Phreak, Major Havoc, y Silver Spy; y pertenecían a grupos autodenominados como The Lords of Chaos, Phantom Access Associates, Shadow Brotherhood y The Coalition of Hi-Tech Pirates, entre otros.

Esta tendencia continuó durante el crecimiento de las computadoras personales, donde inclusive la mayoría de los virus eran demostraciones de poderío intelectual y conocimiento tecnológico por parte de los creadores. Algunos de los más famosos, utilizaban esta fama para ser contratados por empresas importantes, dentro de sus áreas de tecnología,

Con la llegada de la World Wide Web, a mediados de los 90's, y el crecimiento de sitios de comercio electrónico y banca electrónica, comenzó a cambiar el perfil del típico hacker. Comenzaron a haber muchas personas que utilizaban el hackeo para obtener una ganancia personal, la cual podía consistir desde beneficios económicos, perpetrar venganzas o contravenir ciertas posiciones filosóficas o políticas. Este hackeo incluía muchos tipos de actividad. Los Hackers obtenían información personal y luego la utilizaban para robar sumas de dinero, se contrataban con empresas para obtener información industrial o propiedad intelectual de la competencia, (en muchas ocasiones primero robaban la información y luego trataban de venderla a la empresa competidora), atacaban sitios bancarios, casinos en línea, etc.

Estos hackers seguían trabajando de manera aislada, generalmente robaban sumas relativamente pequeñas (con algunas excepciones) y en muchos casos eran más inteligentes tecnológicamente hablando que en otros aspectos. Más de uno fue aprehendido por enviar dinero a sus propias cuentas de cheques, con la dirección en la que vivían, o por ir personalmente a recoger dinero obtenido ilegalmente a la misma tienda, durante meses.

Como consecuencia de la explosión de la interconectividad a finales de los 90's y en la década de los 2000's, con la mayoría de las transacciones financieras del mundo yendo por medios electrónicos y el crecimiento geométrico del uso de Internet para adquirir bienes y servicios, el perfil del hacker tuvo un nuevo cambio, al entrar de lleno el crimen organizado a esta actividad.



Los hackers actuales forman parte de grandes organizaciones criminales internacionales, operando en muchos países.

Existen ejemplos de redes de "negocios" completas, creadas exclusivamente para encubrir actividades criminales, incluyendo pornografía infantil, robo de claves, ataques a empresas y gobiernos, etc. Uno de los más famosos fue la "Russian Business Network" que ocultaba sus actividades detrás de una red supuestamente para personas que querían hacer negocios con Rusia.

Estas organizaciones generan virus y trojanos (programas que se esconden dentro de las computadoras y hacen actividades de daño y espionaje), para obtener información, utilizar las computadoras de las personas para provocar ataques de diversos tipos, y que no sea fácil rastrear de dónde vienen, y además activamente están de manera continua buscando vulnerabilidades en servidores en todo el mundo, sistemas operativos y computadoras personales.

Hace un par de años, Seagate (fabricante de discos duros) tuvo que hacer un anuncio acerca de que algunos de sus discos traían programas maliciosos instalados desde su salida de la fábrica, por lo que las personas que los compraban estaban en riesgo. Nunca quedó 100% claro quién fue la entidad que había infiltrado la fábrica para esconder estos programas en discos que supuestamente estaban en blanco y listos para utilizarse.

También existe razón para sospechar que algunos gobiernos a nivel mundial están generando sus propios virus y programas de espionaje. Ha habido acusaciones de que los gobiernos lo hacen no sólo para obtener información militar y política, sino también para hacer robos y obtener recursos financieros.

Las redes sociales actuales, de todos tipos, no están exentas de actividades criminales. Es muy importante, por ejemplo, educar a los niños y adolescentes acerca de la existencia de personas maliciosas y criminales que recorren todas las redes sociales en búsqueda de víctimas.

Al igual que los piratas de siglo 18, los hackers de los 90's tenían cierto glamour y romanticismo. Muchos de ellos inclusive, nunca obtuvieron un centavo ilegal de sus actividades. Tristemente, los hackers actuales son un elemento más del crimen organizado que tanto ha dañado al mundo en este siglo.

A medida que la tecnología avanza, cada vez hay mayor incentivo para que las organizaciones criminales busquen infiltrar sistemas. Por otra parte, también están habiendo mejoras en la seguridad, desde el diseño mismo de los sistemas operativos.

Es claro que en el futuro, habrá mucho mejor seguridad en redes de comunicación, pero la carrera entre los atacantes y los defensores continuará, con triunfos para ambos bandos.

Los riesgos de las redes sociales

Por Srikan Emmanuel Ruiz Mora
Chief Information Security Officer
KIO Networks

Las redes sociales en México han sido un gran éxito, a tal grado que 4 de los 10 sitios más visitados del país son portales de redes sociales (facebook, HI5, Twitter, etc.). Asimismo, existen al menos 18 millones de cibernautas en México inscritos a una red social. Dentro de estas redes sociales los usuarios comparten con el mundo mucho más que fotografías y videos, ya que dentro del portal de cada usuario se almacenan datos personales como nombre, edad, lugar y fecha de nacimiento, lugar de residencia, etc.

A simple vista, esta información podría no tener relevancia, pero ¿se han puesto a analizar cuál es la información que el buzón de correo nos solicita cuando queremos recuperar la contraseña? ¿O qué datos nos pide el banco cuando quiere confirmar nuestra identidad vía telefónica? Por poner un ejemplo, cuando un usuario quiere recuperar la contraseña de su buzón de correo, la mayoría de los portales nos dan dos opciones; nos pueden enviar la contraseña a una cuenta de correo electrónico alterna o, mejor aún, podemos proporcionar información para crear una nueva contraseña y, para la fortuna de todos, generalmente nos piden 3 datos: el lugar donde fue creada la cuenta, código postal y la respuesta a una pregunta secreta.

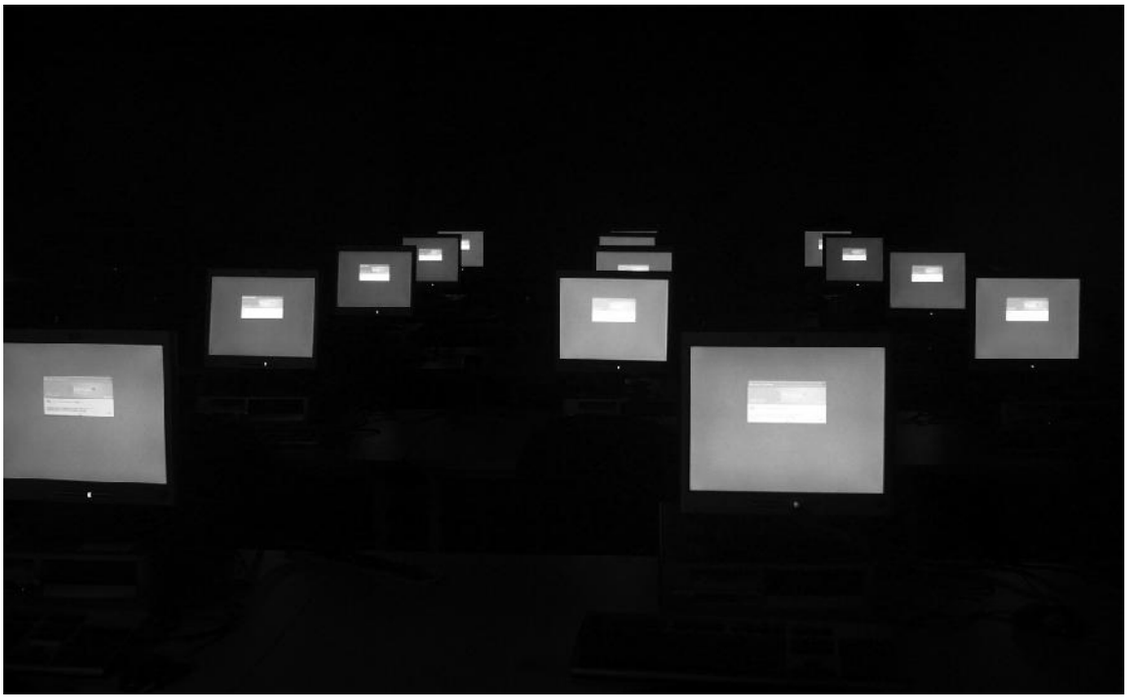
Si nos damos cuenta, con la información que aparece publicada en el perfil del usuario en una de las tantas redes sociales, podemos contestar 2 de las 3 preguntas, o por qué no, con un poco de suerte y paciencia navegando por el portal del usuario podemos encontrar la tan deseada respuesta a la pregunta secreta del usuario, considerando que la gente en ocasiones utiliza como pregunta secreta el nombre de su primer mascota, el nombre o profesión de algún familiar, fechas de viajes o acontecimientos importantes, etc. Éste tipo de información, muchas veces es el que la gente acostumbra a subir en este tipo de sitios.

El problema de la recuperación de la contraseña del correo electrónico es sólo uno de la larga lista de aplicaciones que utilizan estos datos para dar acceso a los usuarios a información confidencial y, desafortunadamente, este problema se vuelve crítico cuando esta misma información es usada para acceder a cuentas de correo o portales en Internet, con información o recursos críticos para una compañía. Esto no es un caso aislado; desafortunadamente gran parte de los ataques efectuados han tenido como base la ingeniería social o recopilación de información como en el ejemplo anterior.

Un tema muy comentado en las últimas semanas fue el caso de Twitter, una de las más grandes redes sociales, la cual fue "hacheada" utilizando una contraseña obtenida de un mail dentro del buzón de correo personal de uno de los desarrolladores del mismo Twitter. El atacante pudo ingresar a través de recuperar la contraseña del usuario, utilizando información personal del mismo almacenada en su perfil de Twitter.

¿Qué significa esto?.- Que al día de hoy nuestros usuarios no conocen los riesgos a los que están expuestos, no sólo en Internet, sino a los riesgos asociados a su puesto y la información confidencial que manejan.

En el caso de Twitter, recordemos que utilizaron una contraseña encontrada en el buzón de correo de un desarrollador. ¿Qué significa esto? Que este usuario utilizaba al menos la misma contraseña para más de una aplicación, lo cual fue validado por el atacante cuando pudo acceder a varios sitios de Twitter con el



nombre y password del usuario. Este ataque es uno de tantos posibles ejemplos, que muestran cómo tener un esquema de seguridad perimetral basado en FWs, IDS, IPS, equipos de filtrado, control de identidades, etc., puede ser insuficiente, ya que estos equipos poco o nada pueden hacer en contra de un acceso válido proporcionado por la persona incorrecta.

Esto no es de extrañarse. El 98% de los usuarios utilizan la misma contraseña para acceder a sus recursos. En la mayoría de las ocasiones esta contraseña no tiene la robustez necesaria y creo que mejor no hablamos de la periodicidad con la cual es actualizada.

¿Cómo podemos evitar esto? ¿Es posible prevenir ataques del tipo ingeniería social a nuestros usuarios? La respuesta es sí. La forma en la cual podemos hacer esto es concientizando a nuestros usuarios, haciéndoles saber cuáles son los posibles riesgos que se le pueden presentar y qué hacer en caso de que esto suceda. Asimismo, es necesario implementar las políticas y procedimientos necesarios que refuercen el perímetro de seguridad de la compañía.

Es por eso que la implementación de políticas y procedimientos es fundamental, lo cual no se limita a sólo darle un curso al usuario, hacerle que lea y firme una política de seguridad y listo. No, debe existir un seguimiento por parte del área de seguridad de la empresa para validar que las políticas y procedimientos se están llevando a cabo; esta área debe cerciorarse de que el usuario conoce, entiende y aplica las políticas de la empresa, los riesgos y sanciones que pueden existir y, asimismo, asegurarse de que el usuario tenga retroalimentación de los nuevos riesgos que surgen día con día.

Regresando a las redes sociales, el mensaje no es dejar de usarlas, sino tener cuidado en qué tipo de información subimos y, de esta misma, cuál queremos que sea visible al mundo o a nuestro circulo de "amigos y/o conocidos", o de cuáles detalles de nuestra vida personal queremos que se enteren, ya que finalmente recordemos que esta información se encuentra en Internet y, como ya hemos visto, hasta estos sistemas son vulnerables a ataques.

Gestión de riesgos de TI utilizando ISO31000 e ISO27005

Por Mario Ureña Cuate
CISSP, CISA, CISM, CGEIT, ISO27001 LA, BS25999 LA
Director General de SecureInformationTechnologies

En la actualidad son cada vez más las organizaciones que están adoptando formas de trabajo basadas en sistemas de gestión tales como ISO9000 para la Gestión de la Calidad e ISO14000 para la Gestión Ambiental, principalmente.

En este entorno, las áreas de TI y Seguridad de la Información no son la excepción y han venido implementando estándares como ISO20000 (Sistema de Gestión de Servicios de TI), ISO38500 (Gobierno Corporativo de TI), BS25999 (Sistema de Gestión de la Continuidad del Negocio) y el popular ISO27001 (Sistema de Gestión de Seguridad de la Información).

Especialmente para estos dos últimos (ISO27001 y BS25999) es necesario realizar un análisis de riesgos en las etapas más tempranas de su implementación, para la definición de los planes de tratamiento de riesgos y en el caso de la BS25999, para la identificación y selección de estrategias de recuperación.

Sin embargo, cuando las organizaciones se enfrentan a la hoja en blanco para el desarrollo del análisis de riesgos se encuentran en un campo de estudio que se encuentra en proceso de madurez y que se puede realizar de muchas formas diversas. El principal objetivo de estándares como el ISO31000 y el ISO27005 es establecer los marcos de referencia generales que sirvan de base para ejecutar el proceso de gestión de riesgos.

EL FUTURO DE LA GESTIÓN DE RIESGOS CON ISO 31000

Con el fin de establecer las guías y principios generales para la gestión de riesgos sin importar su naturaleza, nivel y complejidad, la ISO (International Organization for Standardization) se encuentra trabajando en la publicación del estándar ISO31000, el cual ya se encuentra disponible como borrador y se espera sea liberado en próximas fechas.

Este estándar detalla los principios para la gestión de riesgos, el marco de referencia para la gestión de riesgos y el proceso para la gestión de riesgos.

Son 11 los principios que las organizaciones tienen que reconocer y adoptar:

- La gestión de riesgos crea valor
- Es parte integral de los procesos organizacionales
- Forma parte de la toma de decisiones
- Atiende explícitamente los aspectos de incertidumbre
- Es sistemática, estructurada y oportuna
- Está basada en la mejor información disponible
- Está alineada con el contexto externo e interno de la organización
- Toma en consideración los factores humanos y culturales
- Es transparente e inclusiva
- Es dinámica, iterativa y responde a los cambios
- Facilita la mejora continua en las organizaciones

Aún cuando el marco de referencia para la gestión de riesgos no define un sistema de gestión, ha sido estructurado para que se pueda integrar al sistema de gestión corporativo, e incluye los siguientes elementos:

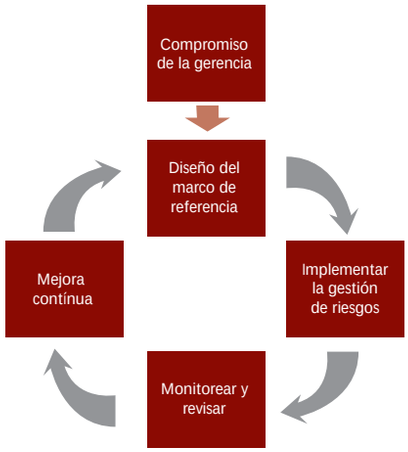


Figura: Marco de referencia para la gestión de riesgos de ISO31000

- Compromiso de la alta gerencia
- Diseño de un marco de referencia para la gestión de riesgos (Generalmente en la etapa Plan/Planear)

  - Entendimiento de la organización y su contexto
  - Política de gestión de riesgos
  - Integración dentro de los procesos de la organización
  - Responsabilidad
  - Recursos
  - Establecer mecanismos de comunicación y reporte internos
  - Establecer mecanismos de comunicación y reporte externos

- Implementar la gestión de riesgos (Generalmente en la etapa Do/Hacer)

  - Implementar el marco de referencia para la gestión de riesgos
  - Implementar el proceso de gestión de riesgos

- Monitorear y revisar el marco de referencia (Generalmente en la etapa Checar/Verificar)
- Mejora continua del marco de referencia (Generalmente en la etapa Act/Actuar)

El proceso para la gestión de riesgos contempla los siguientes elementos:

Comunicación y consulta.- Se debe mantener comunicación y consulta con las partes interesadas tanto internas como externas durante todas las etapas del proceso de gestión de riesgos. El estándar recomienda el desarrollo de un plan de comunicación en alguna de las fases iniciales de la gestión de riesgos.

Establecimiento del contexto.- La organización debe definir los parámetros internos y externos que se deben tener en consideración cuando se gestiona el riesgo, así como el alcance y los criterios de evaluación que se utilizarán para el resto del proceso. Para esta etapa se deben tomar en consideración los requerimientos legales y regulatorios, así como los aspectos culturales, políticos, tecnológicos, financieros, ambientales, etc.

Análisis y evaluación de riesgos (Assessment).- Esta etapa incluye la identificación, análisis, evaluación y tratamiento de riesgos.

Identificación de riesgos.- La organización debe identificar fuentes de riesgo, áreas de impactos, eventos y sus causas, así como sus posibles consecuencias. El objetivo principal de esta etapa es generar una lista de riesgos basándose en los eventos que pudieran mejorar, impedir, degradar o demorar el cumplimiento de los objetivos de la organización. Es recomendable que esta etapa se realice de forma exhaustiva, ya que los riesgos que no se identifiquen en ella no serán considerados en las etapas subsecuentes.

Análisis de riesgos.- Esta etapa tiene como fin el entendimiento de los riesgos. Implica la consideración de las causas y fuentes de riesgo, sus consecuencias positivas y/o negativas y la posibilidad de que esas consecuencias pudieran ocurrir. Se deben tomar en cuenta los controles de riesgo existentes y su efectividad.

El análisis de riesgos se puede ejecutar en diferentes niveles de detalle, dependiendo de los riesgos, el propósito del análisis, así como la información, datos y recursos disponibles. El análisis puede ser cualitativo, semi-cuantitativo, cuantitativo o una combinación, dependiendo de las circunstancias.

En la práctica, es común que se utilice primero un enfoque cualitativo para obtener un indicador general e identificar los riesgos más relevantes.

Evaluación de riesgos.- El propósito de esta etapa es asistir en la toma de decisiones, a través de los resultados del análisis de riesgos, identificando y priorizando aquéllos que requieren tratamiento.
La evaluación de riesgos implica la comparación entre el nivel de riesgo encontrado durante el proceso de análisis contra el criterio de riesgos establecido en el contexto.

Tratamiento de riesgos.- Esta etapa consiste en seleccionar una o más opciones para modificar los riesgos y la implementación de dichas opciones. Las opciones de tratamiento de riesgos no son necesariamente excluyentes entre ellas. Las opciones de tratamiento que propone el ISO31000 son:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad asociada al riesgo.
- Identificar una oportunidad al decidir iniciar o continuar con una actividad que crea o incrementa el riesgo.
- Remover la fuente del riesgo.
- Cambiar la naturaleza y magnitud de la posibilidad de ocurrencia.
- Cambiar las consecuencias.
- Compartir el riesgo con un tercero(s) y
- Retener el riesgo por elección.

Monitoreo y revisión.- El monitoreo y la revisión debe ser una parte planeada del proceso de gestión de riesgos y la responsabilidad para su realización debe estar

claramente definida. Los resultados de estas actividades deben ser utilizados para mejorar el proceso de gestión de riesgos de la organización.

Uno de los principales motivos para el desarrollo de este estándar ISO31000, ha sido el contar con los principios y guías generales para la gestión de riesgos, permitiendo el desarrollo de estándares más específicos para la atención de diferentes tipos de riesgo, como es el caso de los riesgos de seguridad de la información a través del ISO27005.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN CON ISO27005

El estándar ISO27005 se ha desarrollado para apoyar a las organizaciones que han decidido implementar un Sistema de Gestión de Seguridad de la Información basado en ISO27001 e ISO 27002, sin embargo, debemos tener muy claro que:

1.- No es mandatorio el cumplimiento con ISO27005 para efectos de certificación en conformidad con ISO 27001 y

2.- Cualquier organización que desee gestionar sus riesgos de seguridad de la información puede utilizar este estándar, aun cuando no cuente con un Sistema de Gestión de Seguridad de la Información basado en ISO27001.

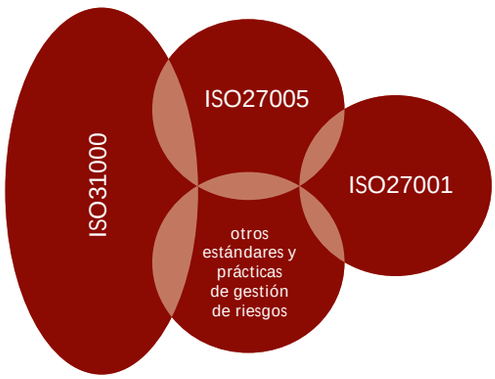


Figura: Integración de estándares para la gestión de riesgos con ISO27001

Este estándar propone un proceso similar al de ISO31000, sin embargo, durante la etapa de identificación de riesgos, el ISO27005 requiere que se realice la identificación de activos, amenazas, controles existentes, vulnerabilidades y consecuencias, mientras que la estimación de riesgos requiere la evaluación de las consecuencias y la posibilidad de ocurrencia de los incidentes.

ISO27005 detalla cuatro tipos de tratamiento de riesgos: Reducir el riesgo, Retener el riesgo, Evitar el riesgo y Transferir el riesgo. A diferencia del ISO 31000, éste no describe la posibilidad de explotar o aprovechar el riesgo.

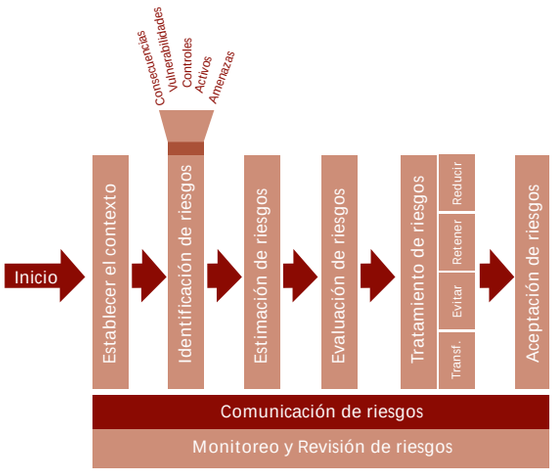


Figura: Conceptualización del proceso de gestión de riesgos de ISO27005

Cada vez es más común que las organizaciones cuenten con una función encargada de la gestión de riesgos o GRC a nivel corporativo y es importante que los profesionales de seguridad de la información integremos los esfuerzos que corresponden a nuestra especialidad con los que se realizan a nivel corporativo, conociendo los modelos de gestión de riesgos emergentes y la forma en que éstos se interrelacionan.

Hacia una cultura de la Seguridad de la Información

Por Pedro F. Solares Soto
Maestría en Ingeniería de Sistemas Empresariales
de la Universidad Iberoamericana

Existen diversos enfoques de la definición de la seguridad de la información. En términos generales, es factible entender la seguridad como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. Es garantizar que los recursos informáticos de una empresa estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos.

En la mayoría de los estudios han encontrado que el escaso conocimiento de los usuarios es la principal causa individual de las brechas de seguridad en los sistemas de información (redes). Una gran cantidad de empleados olvidan sus contraseñas para acceder a los sistemas de cómputo o permiten a sus colegas que las utilicen, lo cual pone en riesgo al sistema. Los intrusos malintencionados que buscan acceso al sistema, en ocasiones engañan a los empleados para que les proporcionen las contraseñas, fingiendo que son miembros legítimos de la organización y requieren información. La disciplina del conocimiento que estudia este tipo de problemática es la Ingeniería Social.

A manera de ejemplo "hipotético", digamos que un empleado prestó (o extravío) su contraseña y la competencia accedió a los planes estratégicos de la empresa. Mencionemos otro caso, en donde un alto directivo bajó archivos de Internet que estaban infectados con un virus que paralizó la red de la organización por días. Las organizaciones y sus redes de información (informáticas o no), cada día se enfrentan a una gran variedad de amenazas de seguridad de la información como: fraudes por computadora, virus, delitos informáticos, robo de información interna, hackers, sabotaje, espionaje y vandalismo, entre otros. Estas amenazas crecen a la par de los adelantos tecnológicos, ocasionando que sea más complicada la forma de detectarlos.

La problemática es más compleja por las estructuras ineficientes de seguridad de la información que tienen una gran cantidad de empresas a nivel mexicanas y extranjeras, y porque no existe conocimiento relacionado con la planeación de un programa de seguridad integral que proteja los recursos informáticos de las amenazas actuales. La seguridad de la información tiene por objetivo proteger el activo básico (información) de la empresa, respecto a una amplia gama de amenazas, con el fin de minimizar los riesgos y asegurar que la rentabilidad o relación costo/beneficio sean los mejores. Es la información el factor primordial a proteger, resguardar y recuperar dentro de las redes empresariales.

La tecnología no es el único aspecto clave en la seguridad y el control de los sistemas de información. La tecnología ofrece una base, pero ante la falta de políticas de administración inteligentes, la mejor tecnología, incluso, puede ser anulada. Los expertos consideran que más de 90 por ciento de los ciber ataques exitosos se podrían haber evitado con la tecnología disponible en ese momento. La falta de atención sobre el factor humano, permitió que estos ataques fueran contundentes. Se recomienda que el enfoque sea a la par cultural y tecnológico.

Por lo general, se tiene la percepción de que las amenazas a la seguridad de una empresa provienen del exterior de la organización. No obstante, los empleados de una empresa plantean serios problemas de seguridad. El personal suele tener acceso a información privilegiada y, si existen procedimientos de seguridad ineficientes, pueden tener la oportunidad de escudriñar en todos los sistemas de la organización sin dejar huella. En

otro porcentaje considerable de los casos, los usuarios finales introducen errores al ingresar datos incorrectos y/o deficientemente capturados al no seguir las instrucciones apropiadas para el procesamiento de datos y el uso del equipo de cómputo.

De ahí que sea fundamental crear una cultura de seguridad entre los empleados, los directivos y dueños de las empresas, para que lo asuman como factor clave en la competitividad y desarrollo de su labor cotidiana en el centro de trabajo. La cultura desarrollada por la empresa no tiene que afectar el desempeño y la productividad laboral de los empleados. Hay que incidir en un cambio en la cultura de la organización que permita a futuro incorporar la seguridad informática como parte de la actividad cotidiana de cada uno de los individuos.

Es factible afrontar el problema de nivel cultural con el proceso de educar a los usuarios y a las personas clave al interior de las empresas (directores de departamento, jefes de área, coordinadores) si se les imparten: inducciones, capacitaciones, seminarios, talleres y cursos, entre otros.

La consciencia de seguridad en informática en México se sigue incrementando. Sin embargo, este avance es más lento de lo deseable. Es reducido el número de personas que conceptualiza que la seguridad de la información está íntimamente ligada a los procesos y a las políticas. Así, un plan de cultura dirigida a la seguridad de la información tiene que ser completo e incluir las políticas sobre aspectos de seguridad, reuniones con los grupos objetivos y contar con una metodología adecuada con fundamento en las Certificaciones Profesionales Internacionales y los estándares a nivel mundial.

Al implementar un programa de cultura de la seguridad de la información en una organización, es necesario conceptualizar que su aplicación es dinámica, redefiniendo significativamente las definiciones y documentos para ser aplicados constantemente día tras día. Además, hay que crear indicadores y/o parámetros para medir los resultados del programa. Existen algunos obstáculos en la gran mayoría de las empresas para implementar un plan de cultura para la seguridad. Sin ser una lista exhaustiva y jerárquica, se mencionan los siguientes obstáculos: no reconocer que la seguridad es labor de todos los empleados de la organización; la adquisición de una nueva tecnología; la falta de un seguimiento adecuado al programa de cultura de la seguridad de la información; el no recibir apoyo de la alta gerencia; nuevos modus operandi de los delincuentes; los empleados reacios a cambiar paradigmas, entre otros.

Las organizaciones actualmente han comprendido la importancia de generar una seguridad contra aquellos agentes agresores que buscan constantemente aprovechar las vulnerabilidades que los sistemas informáticos e infraestructura (red) presentan. Es interesante comprender que por muy robustos que sean los sistemas de seguridad en las organizaciones, no servirían de nada si el eslabón más débil de la cadena (el usuario de la información) está desvinculado de la parte fundamental del programa de cultura de seguridad.

Teniendo en consideración las "no gratas experiencias" y aquellos "casos de terror" relacionados con la seguridad de la información, es recomendable desarrollar un plan de seguridad integral que sustente sus procesos de negocio en el uso correcto de las Tecnologías de la Información, porque si la empresa carece de cultura para aprovechar la tecnología, aumenta la vulnerabilidad de la organización.

ESTUDIO DE PERCEPCIÓN
SEGURIDAD DE LA INFORMACIÓN MÉXICO 2010

Con la finalidad de tener un panorama de la evolución del mercado de seguridad en informática en México, así como un conocimiento acerca de cómo este concepto se va incorporando a la vida personal y dinámica de las empresas de nuestro país, este estudio, desde su primera edición en 2004, está siendo actualizado y editado anualmente.

En estos primeros meses, se está efectuando el diseño, planteamiento metodológico y definición de patrocinios, para el desarrollo de la investigación para la edición de 2010.

Para mayor información, comuníquese a los siguientes teléfonos en la Ciudad de México:

(55) 5286 -1839
(55) 5286 - 6906
market@jfs.com.mx

www.jfs.com.mx

AMIPCI

AHK Deutsch-Mexikanische Industrie- und Handelskammer
Cámara Mexicano-Alemana de Comercio e Industria | CAMEXA

CANIETI www.canieti.org

CISCO