Estudio de Percepción

Seguridad en Informática

México 2004

JFS

JOINT FUTURE SYSTEMS

CAMEXA

CANIETI

EL UNIVERSAL

IRON MOUNTAIN

KIO NETWORKS

Política digital

Sun microsystems

symantec

Vilsa

CAMEXA
German Centre
Centro Alemán
Avenida Santa Fe 170, 1-4-10
Lomas de Santa Fe
01210, México, D.F.
Tel. (55) 1500-5900
www.camexa.com.mx

KIO NETWORKS
Prol. Paseo
de la Reforma 5287
Cuajimalpa
05000 México, D.F.
Tel. (55) 8503-2600
www.kionetworks.com

CANIETI
Culiacán 71
Col. Hipódromo Condesa
06100 México, D.F.
Tel. (55) 5264-0808
www.canieti.org

POLÍTICA DIGITAL
Cuautla 10
Col. Condesa
06140 México, D.F.
Tel. (55) 5211-0010
www.politicadigital.com.mx

EL UNIVERSAL
Bucareli 8
Col. Centro
06040 México, D.F.
Tel. (55) 5709-1313
www.eluniversal.com.mx

SUN MICROSYSTEMS
Prol. Reforma 600-210
Col. Peña Blanca Santa Fe
01210 México, D.F.
Tel. (55) 5258-6100
http://mx.sun.com

IRON MOUNTAIN
Hidalgo 1911 - PB
esq. Baudelaire
Col. Obispado
64060 Monterrey, N.L.
Tel. (81) 8122-0500
www.ironmountain.com

SYMANTEC
Blvd. Adolfo Ruiz Cortines
3642 piso 8
Col. Jardines del Pedregal
01900 México, D.F.
Tel. (55) 5481-2600
www.symantec.com

JOINT FUTURE SYSTEMS
Av. México 19-701
Col. Condesa
06100 México, D.F.
Tel. (55) 5286-1839
www.jfs.com.mx

TÉCNICA COMERCIAL VILSA
Montecito 38 piso 22
Ofic. 21 y 22
Col. Nápoles
03810 México, D.F.
Tel. (55) 5488-0824
www.vilsa.com.mx

Estudio de Percepción
Seguridad en Informática México 2004

Si bien las fronteras entre países siguen siendo elementos delimitadores de ciertos atributos, como son propiedad territorial, disponibilidad de recursos, formas de pensar y maneras de hacer las cosas, el mundo es uno solo en materia de información. La dinámica de la vida moderna se caracteriza por una necesidad creciente de administración e intercambio de datos, lo que ha dado lugar a la más extensa red de comunicación que el Ser Humano hubiera podido imaginar y en donde el uso intensivo de tecnología es un factor indispensable.

El valor de la información ha ido tomando una posición de altísima relevancia en todos los ámbitos: en los negocios, en el gobierno, en la educación, en la vida personal. Su pérdida o el uso inadecuado de la misma, puede repercutir en daños de diversas magnitudes, desde el desperdicio de valiosas horas de trabajo, el deterioro de una reputación o la disminución de oportunidades de venta, hasta la pérdida de millones de pesos en activos o como consecuencia del espionaje industrial, por ejemplo. Desde los principios de los años 90's, en los cuales jóvenes atacaron con éxito las empresas de telefonía en Estados Unidos, pasando por los ataques directos a los sistemas de empresas y organismos gubernamentales de finales de los 90´s, hasta nuestros días, con innumerables amenazas cibernéticas (propagación de programas dañinos, saturación intencional de sistemas, recopilación de información sin permiso del propietario), en un entorno social y laboral en el cual las empresas y los individuos literalmente no pueden funcionar sin conexiones electrónicas, la seguridad en informática sigue creciendo en importancia. Todos estos acontecimientos han provocado una mayor conciencia alrededor de la Seguridad en Informática y de la importancia de desarrollar planes de protección de manera anticipada. Pero, ¿Qué está pasando en México? ¿Hasta dónde ha penetrado esta conciencia? ¿Qué tanto conocen los usuarios corporativos e institucionales acerca de estos riesgos y de cómo enfrentarlos?

Ante estas cada vez más frecuentes muestras de vulnerabilidad informática a nivel mundial, se planteó la realización de un Estudio que permitiera conocer, por un lado, la opinión de los líderes de la industria de TI respecto del mercado de Seguridad en Informática en México y, por el otro, los niveles de conciencia que los empresarios y directivos de diversas organizaciones públicas y privadas de nuestro país, tienen acerca de la importancia de contar con planes estructurados de Seguridad en Informática, así como el grado de conocimientos con los que cuentan acerca de las soluciones existentes para proteger su información y mantener la continuidad de sus operaciones.

Joint Future Systems, S.C., organización con más de 6 años de experiencia desarrollando Investigación de Mercados para la industria de Tecnología de la Información, encabezó este proyecto con el propósito de fomentar la cultura de Seguridad entre empresas e instituciones, e impulsar, al mismo tiempo, el mercado de productos y servicios especializados. La realización de los estudios y la producción de este documento, fueron posibles gracias a la colaboración de importantes empresas que comparten el interés por hacer extensiva esta conciencia a diferentes niveles de la sociedad, y por ofrecerles una herramienta de orientación y consulta que, paralelamente, promueva un mayor desarrollo de este mercado en todo México. Estas empresas fueron, en orden alfabético:

Empresas patrocinadoras

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

Cámara Nacional de la Industria Electrónica de Telecomunicaciones e Informática

El Universal, Compañía Periodística Nacional

Iron Mountain

Joint Future Systems, S.C.

Kio NetWorks México

Política Digital, una publicación de Grupo Nexos

Sun Microsystems de México, S.A. de C.V.

Symantec de México, S.A. de C.V.

Técnica Comercial Vilsa, S.A. de C.V.

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

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

CONTENIDO

I. Introducción

Para tener un panorama completo de lo que está sucediendo alrededor de la Seguridad en Informática en México, era necesario conocer los puntos de vista de diferentes sectores. Evaluar el grado de conocimiento y la percepción que existe respecto de las diferentes áreas de la Seguridad en Informática en la sociedad, requería hacer un levantamiento de información entre usuarios corporativos e institucionales, y entre los responsables de la implementación de proyectos informáticos en las organizaciones.

Esta perspectiva se ve enriquecida con la opinión y puntos de vista de proveedores líderes en el mercado de soluciones de Tecnología de la Información (TI). Así, se decidió la realización de dos estudios complementarios entre si, así como la inclusión, al final del documento, de artículos escritos por algunos de los patrocinadores, con información sobre seguridad en informática útil para los lectores.

A) Estudio de Mercado entre empresas y áreas usuarias de TI.
B) Estudio de opinión y análisis con 20 proveedores líderes del mercado de soluciones TI, en diversas rubros de la seguridad en informática.
C) Artículos de interés, relacionados con seguridad en informática.

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

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

Se describen objetivos, contenido y metodología, en el Capítulo II.

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

Cuestionario estructurado con ejecutivos y directivos de las empresas líderes de soluciones informáticas en nuestro país.

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. Conocer 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 (Relación jerárquica de conceptos).
4. Conocer la percepción que tienen 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. Crear una herramienta que permita fomentar la conciencia y desmitificación de la Seguridad en Informática, apoyando las labores educativas del país a nivel corporativo e institucional.
6. Crear un entorno que impulse el crecimiento del mercado de productos y servicios de seguridad, así como la correcta implementación de soluciones especializadas.

Ámbito de estudio

Seguridad Física

- Seguridad física de las instalaciones.
- Protección física de la información.
- Integridad de los datos.
- Posibilidades de extracción.

Seguridad frente a agresores externos

- Control de acceso al inmueble.
- Control y supervisión de visitantes.
- Manipulación no autorizada de la información o extracción, por medios magnéticos o comunicaciones de datos.

Seguridad frente a agresores internos

- Software utilizado y estructura de derechos y privilegios.
- Controles de acceso a los servicios informáticos.
- Controles de acceso a diferentes áreas de las instalaciones.
- Monitoreo de las acciones realizadas.
- Análisis del grado de satisfacción del personal con su trabajo, niveles de responsabilidad y compromiso.
- Análisis de políticas y reglas para el manejo de la información. Establecimiento y comunicación de sanciones.

Plan de Recuperación en caso de Desastre (DRP)

Diseño de acciones preventivas, para poder utilizar equipos y/o procedimientos alternos en casos de emergencia, su difusión entre el personal y determinación de tiempos para llevarlas a cabo.

II. Investigación entre empresas y áreas usuarias de TI

Objetivos del estudio

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

Metodología

Método de investigación

Encuestas telefónicas.

Las encuestas fueron realizadas en el periodo que abarca del 12 de abril al 29 de junio de 2004, y se llevaron a cabo en 2 etapas, como se describe:

Etapa 1. Calificación de los candidatos a ser encuestados e invitación a participar.

Una vez contactados los perfiles necesarios, más del 60% de las personas que calificaron estuvieron dispuestas a contestar la encuesta en ese mismo momento. Algunos dieron cita para una llamada telefónica posterior, entrevista personal o solicitaron el envío del cuestionario por correo electrónico.

Etapa 2. Realización de encuesta con las personas que calificaron y no contestaron el cuestionario durante la llamada de primer contacto.

Instrumento de medición

Cuestionario estructurado.

Características de la muestra

Perfil de los entrevistados

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

Cuotas por área organizacional

Áreas de Sistemas	30%
Otras áreas	70%

Campo de muestreo

Se utilizaron diversas bases de datos públicas.

Tamaño de la muestra

1,200 entrevistas efectivas con ejecutivos y gerentes de 923 organizaciones, concretadas a partir de procedimientos aleatorios de selección sobre el campo de muestreo.

Codificación de respuestas

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

Resultados

Composición de la muestra

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

Tabla 1

Composición de la muestra por SECTOR		
Giro	**Total**	**Proporción**
Servicios	572	47.7%
Comercio	256	21.3%
Manufactura	165	13.8%
Gobierno	113	9.4%
Instituciones Educativas	28	2.3%
Comunicaciones	19	1.6%
Construcción	19	1.6%
Transportación	17	1.4%
Cámara / Asociación	11	0.9%
Total general	**1200**	**100.0%**

Tabla 2

Composición de la muestra por SEXO		
Sexo	**Total**	**Proporción**
Hombre	911	75.9%
Mujer	289	24.1%
Total general	**1200**	**100.0%**

Tabla 3

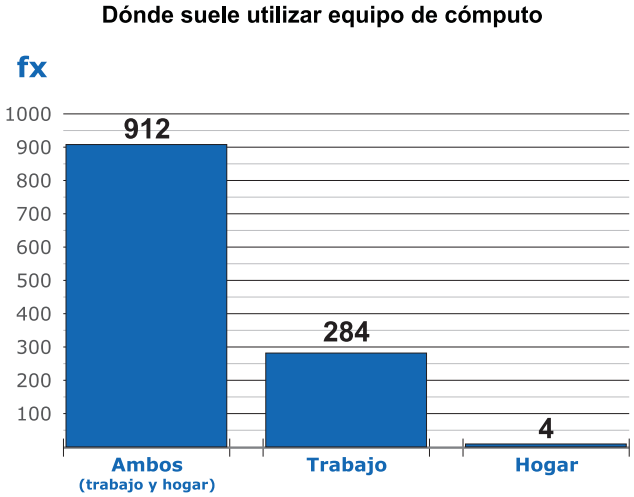
Composición de la muestra por PUESTO / ÁREA		
Puesto / Área de trabajo	**Total**	**Proporción**
Sistemas	360	30.0%
Admón./Finanzas	290	24.2%
P/VP/DG/Dueño/Estrategia *	171	14.3%
Producción/Operaciones	144	12.0%
Mkt./Publicidad	131	10.9%
Ventas	104	8.7%
Total general	**1200**	**100.0%**

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

Lugar donde utilizan equipo de cómputo

La Gráfica 1 presenta la distribución de la muestra, de acuerdo al lugar en donde utilizan equipo de cómputo, en la cual se puede observar que la gran mayoría (76%) utiliza computadoras tanto en casa como en el trabajo, 23.7% únicamente en el trabajo, y sólo el 0.3% lo utiliza en el hogar y nunca en el trabajo.

GRÁFICA 1



Qué se entiende por "Seguridad en Informática"

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

Se registraron todas las respuestas emitidas por los entrevistados, quienes por lo regular mencionaron más de una opción (1.9 respuestas promedio por entrevistado). La frecuencia de las respuestas ya codificadas, pueden apreciarse en la Tabla 4 y la Gráfica 2.

TABLA 4

Qué se entiende por Seguridad en Informática
Tabla de frecuencias

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Acceso autorizado	460	109	569	54.8%	30.3%	38.3%	9.1%	47.4%
Protección contra virus	415	64	479	49.4%	17.8%	34.6%	5.3%	39.9%
Integridad / Confiabilidad de la información	196	131	327	23.3%	36.4%	16.3%	10.9%	27.3%
Respaldo de información	131	64	195	15.6%	17.8%	10.9%	5.3%	16.3%
Transmisión segura de datos	72	52	124	8.6%	14.4%	6.0%	4.3%	10.3%
Políticas adecuadas	86	37	123	10.2%	10.3%	7.2%	3.1%	10.3%
Cuidado de los equipos	72	39	111	8.6%	10.8%	6.0%	3.3%	9.3%
Manejo adecuado de herramientas	70	-	70	8.3%	-	5.8%	-	5.8%
Disponibilidad de la información	18	37	55	2.1%	10.3%	1.5%	3.1%	4.6%
Protección contra hackers	42	-	42	5.0%	-	3.5%	-	3.5%
Uso de software original	30	-	30	3.6%	-	2.5%	-	2.5%
Configuración correcta de los sistemas	-	29	29	-	8.1%	-	2.4%	2.4%
No existe	19	-	19	2.3%	-	1.6%	-	1.6%
Otros	84	42	126	10.0%	11.7%	7.0%	3.5%	10.5%

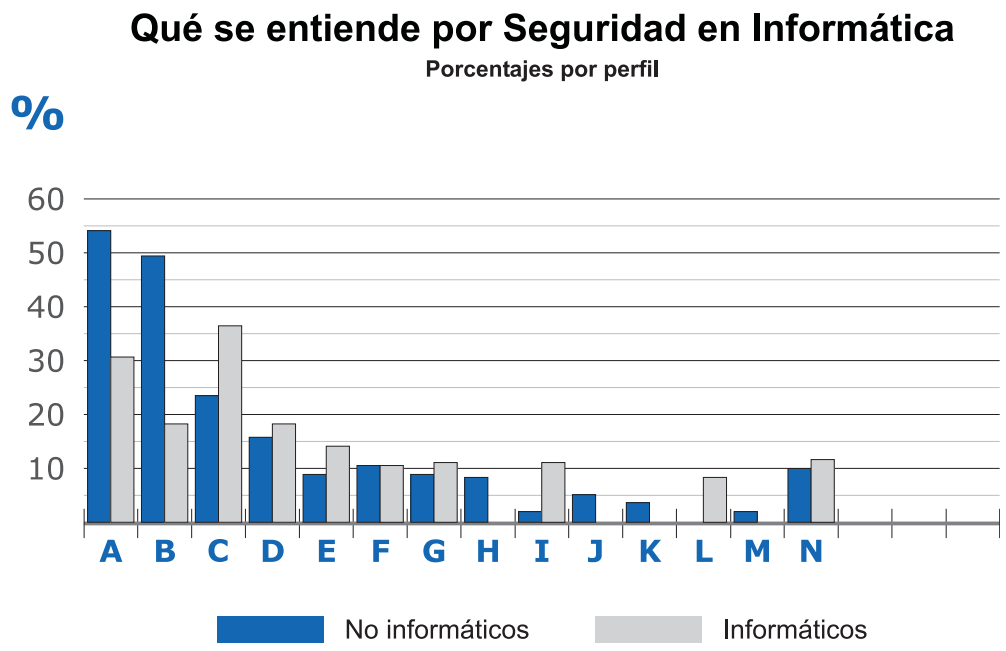
A nivel general de toda la muestra, los conceptos principales asociados a Seguridad en Informática, son el acceso autorizado, la protección contra virus y la integridad y confiabilidad de la información. En cuanto a "Acceso Autorizado", la mayoría de las respuestas hicieron referencia al acceso a los sistemas y a los equipos, aunque unas cuantas se refirieron al acceso a las instalaciones, con respuestas como "Contraseñas", "Control de intrusos", "Confidencialidad de la información", etc.

Es notorio que para los "Informáticos", tiene más peso la Integridad y confiabilidad de la información, que cualquier otro rubro, incluyendo los accesos no autorizados.

De manera notoria, la protección contra virus está asociada al concepto de seguridad, con mucha mayor frecuencia entre los "No informáticos" que entre los "Informáticos", habiendo sido mencionada de manera espontánea por casi la mitad del primer grupo, contra un 17.8% del segundo.

Para los "No informáticos", la configuración correcta de los sistemas no tiene una posición relevante como factor de Seguridad en Informática.

Para una proporción de los "No informáticos" (3.6%), el uso de software original tiene implicaciones en beneficio de la Seguridad en Informática.



Gráfica 2

A Acceso autorizado
B Protección contra virus
C Integridad / Confiabilidad de la información
D Respaldo de información
E Transmisión segura de datos
F Políticas adecuadas
G Cuidado de los equipos
H Manejo adecuado de herramientas
I Disponibilidad de la información
J Protección contra "hackers"
K Uso de software original
L Configuración correcta de los sistemas
M No existe
N Otros

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

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

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

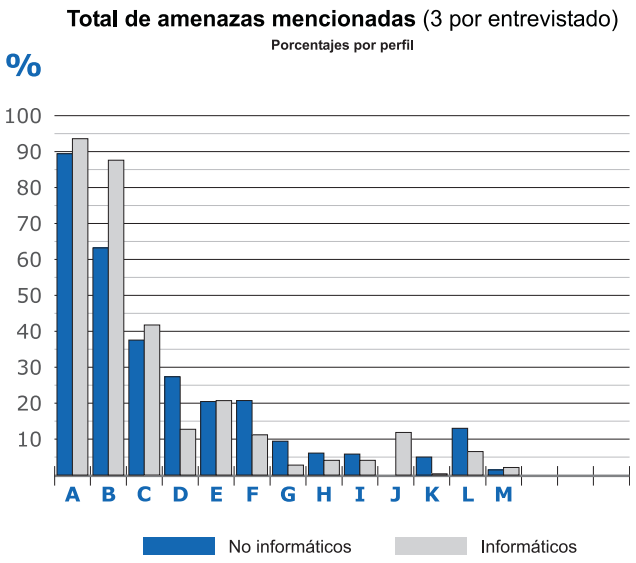
En conjunto, las principales amenazas fueron como se describe en la Tabla 5 y en la Gráfica 3.

TABLA 5

Principales 3 amenazas que ponen en riesgo la seguridad de equipos e información

Tabla de frecuencias

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Virus	753	337	1,090	89.6%	93.6%	62.8%	28.1%	90.8%
Hackers y otros agresores externos	529	315	844	63.0%	87.5%	44.1%	26.3%	70.3%
Desconocimiento	314	151	465	37.4%	41.9%	26.2%	12.6%	38.8%
Fallas de energía	231	45	276	27.5%	12.5%	19.3%	3.8%	23.0%
Agresores internos	170	73	243	20.2%	20.3%	14.2%	6.1%	20.3%
Negligencia	175	42	217	20.8%	11.7%	14.6%	3.5%	18.1%
Insuficiencia de equipo informático	80	9	89	9.5%	2.5%	6.7%	0.8%	7.4%
Conectividad no controlada	52	15	67	6.2%	4.2%	4.3%	1.3%	5.6%
Extracción de información	50	15	65	6.0%	4.2%	4.2%	1.3%	5.4%
Software deficiente	2	44	46	0.2%	12.2%	0.2%	3.7%	3.8%
Internet	41	1	42	4.9%	0.3%	3.4%	0.1%	3.5%
Falta de cultura en seguridad en informática	24	3	27	2.9%	0.8%	2.0%	0.3%	2.3%
Pérdida de información	25	2	27	3.0%	0.6%	2.1%	0.2%	2.3%
Falta de mantenimiento	24	-	24	2.9%	-	2.0%	-	2.0%
Hardware deficiente	-	20	20	-	5.6%	-	1.7%	1.7%
Daño al disco duro	19	-	19	2.3%	-	1.6%	-	1.6%
Tecnología demasiado compleja	15	-	15	1.8%	-	1.3%	-	1.3%
NS/NC	16	8	24	1.9%	2.2%	1.3%	0.7%	2.0%



GRÁFICA 3

A Virus
B "Hackers" y otros agresores externos
C Desconocimiento
D Fallas de energía
E Agresores internos
F Negligencia
G Insuficiencia de equipo informático
H Conectividad no controlada
I Extracción de información
J Software deficiente
K Internet
L No existe
M Otros

En general existe coincidencia entre ambos grupos ("Informáticos" y "No informáticos"), respecto del orden en el que se dan las frecuencias de respuesta, sobre los conceptos mencionados como amenaza. Para una proporción mayor del grupo de los Informáticos, los agresores internos tienen mayor incidencia en los problemas de seguridad que las fallas de energía, mientras que para los "No informáticos" la proporción se da a la inversa.

Casi todos los entrevistados (89.6 % de los "No informáticos" y 93.6% de los "Informáticos"), mencionaron a los virus como una de las principales amenazas contra la Seguridad en Informática.

La amenaza considerada de mayor riesgo

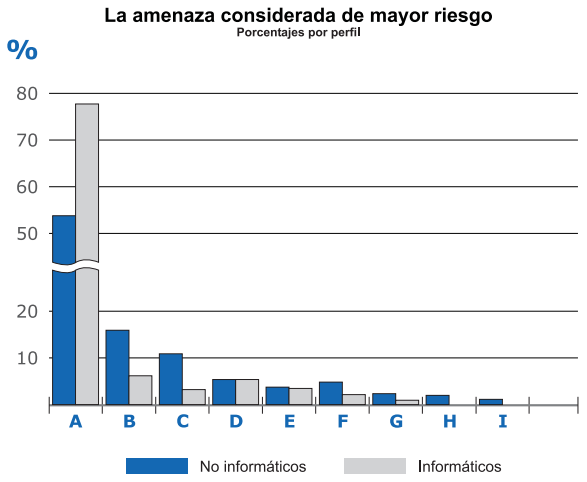
Pregunta complementaria a la anterior: Por favor asigne un número de 1 a 3 a las amenazas que acaba de mencionar, indicando 1 para aquélla que considera más riesgosa y 3 la que dejaría como última prioridad.

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

Tabla 6

La amenaza considerada de mayor riesgo
Tabla de frecuencias

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Virus	450	281	731	53.6%	78.1%	37.5%	23.4%	60.9%
Desconocimiento	140	23	163	16.7%	6.4%	11.7%	1.9%	13.6%
Hackers y otros agresores externos	88	12	100	10.5%	3.3%	7.3%	1.0%	8.3%
Agresores internos	42	18	60	5.0%	5.0%	3.5%	1.5%	5.0%
Negligencia	31	12	43	3.7%	3.3%	2.6%	1.0%	3.6%
Extracción de información	35	8	43	4.2%	2.2%	2.9%	0.7%	3.6%
Fallas de energía	20	6	26	2.4%	1.7%	1.7%	0.5%	2.2%
Daño al disco duro	19	-	19	2.3%	-	1.6%	-	1.6%
Tecnología demasiado compleja	15	-	15	1.8%	-	1.3%	-	1.3%
Total general:	840	360	1200	100.0%	100.0%	70.0%	30.0%	100.0%



Gráfica 4

A Virus
B Desconocimiento
C "Hackers" y otros agresores externos
D Agresores internos
E Negligencia
F Extracción de información
G Fallas de energía
H Daños al disco duro
I Tecnología demasiado compleja

En ambos grupos, "Informáticos" y "No informáticos", la amenaza de mayor riesgo con mayor frecuencia de respuestas es el ataque de virus, seguida por el desconocimiento de los usuarios. Para una proporción mayor del grupo de los "Informáticos", los agresores internos representan una amenaza de mayor riesgo, antes que los "hackers" y otros agresores externos, a diferencia de los "No informáticos", en donde más personas mencionaron a los "hackers" como el riesgo mayor, sobre los agresores internos.

Ninguno de los "Informáticos" mencionó los daños al disco duro ni la tecnología demasiado compleja, como la amenaza de mayor riesgo.

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

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

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

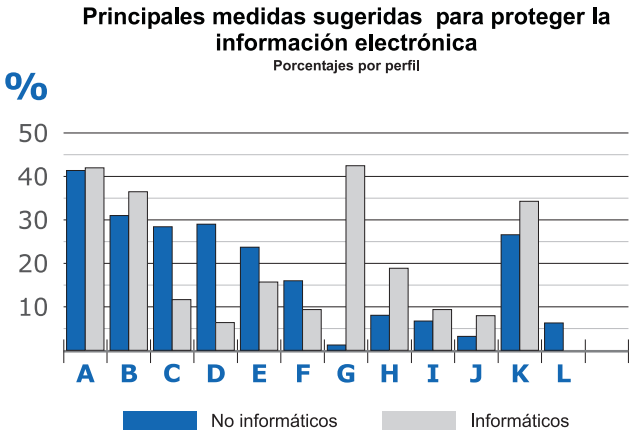
TABLA 7

Principales medidas para proteger la información electrónica

Tabla de frecuencias

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Antivirus	350	152	502	41.7%	42.2%	29.2%	12.7%	41.8%
Políticas / implementación de controles de acceso	263	130	393	31.3%	36.1%	21.9%	10.8%	32.8%
Capacitación adecuada	239	43	282	28.5%	11.9%	19.9%	3.6%	23.5%
Contraseñas	242	24	266	28.8%	6.7%	20.2%	2.0%	22.2%
Respaldar información	201	56	257	23.9%	15.6%	16.8%	4.7%	21.4%
Políticas integrales y una cultura de seguridad en inf.	133	34	167	15.8%	9.4%	11.1%	2.8%	13.9%
Firewalls / Proxy	10	153	163	1.2%	42.5%	0.8%	12.8%	13.6%
Monitoreo y control de sistemas	62	69	131	7.4%	19.2%	5.2%	5.8%	10.9%
Instalaciones físicas adecuadas	56	33	89	6.7%	9.2%	4.7%	2.8%	7.4%
Software seguro / actualizado	28	28	56	3.3%	7.8%	2.3%	2.3%	4.7%
Mantenimiento adecuado de hardware	40	4	44	4.8%	1.1%	3.3%	0.3%	3.7%
Reclutamiento y selección de personal adecuados	31	-	31	3.7%	-	2.6%	-	2.6%
Contar con proveedores confiables	30	-	30	3.6%	-	2.5%	-	2.5%
Sistemas Operativos más seguros	-	29	29	-	8.1%	-	2.4%	2.4%
Implementación correcta de los sistemas	-	27	27	-	7.5%	-	2.3%	2.3%
Uso de biométricos	23	-	23	2.7%	-	1.9%	-	1.9%
Redundancia	-	21	21	-	5.8%	-	1.8%	1.8%
Políticas antipiratería	15	-	15	1.8%	-	1.3%	-	1.3%
Otros	84	42	126	10.0%	11.7%	7.0%	3.5%	10.5%
NS/NC	53	-	53	6.3%	-	4.4%	-	4.4%

Gráfica 5



A Antivirus
B Políticas / implementación de controles de acceso
C Capacitación adecuada
D Contraseñas
E Respaldar información
F Políticas integrales y una cultura de seguridad en informática
G Firewall / Proxy
H Monitoreo y control de sistemas
I Instalaciones físicas adecuadas
J Software seguro / actualizado
K Otros
L NS/NC - No Sabe / No Contestó

Es notorio que los 3 aspectos más importantes para los "Informáticos", como medida de seguridad a implementarse, son el uso de tecnología de control y administración de las telecomunicaciones (firewalls, proxys, etc.), así como el uso de soluciones antivirus y la implementación de políticas y controles de acceso, entre las que se mencionaron el establecimiento de privilegios, restricciones de acceso de personas a las instalaciones, turnos de trabajo bien definidos, acceso limitado a Internet para el personal, sanciones claras, creación de planes de contingencia tipo DRP, etc.

Aunque en menor proporción respecto de los "No informáticos", para los "Informáticos" también son importantes los respaldos de información y la capacitación adecuada, tanto de los administradores de los sistemas, como del personal en general.

A diferencia de los "Informáticos", muy pocos de los entrevistados del grupo de los "No informáticos" mencionaron soluciones tipo Firewall. Las sugerencias más mencionadas por ellos para protección de los sistemas, giraron alrededor de soluciones antivirus, políticas y control de acceso, capacitación y uso de contraseñas, principalmente.

También se observa una mayor preocupación por parte de los "Informáticos" por que existan herramientas que permitan el monitoreo y administración remota de los sistemas.

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

Si bien a grandes rasgos las sugerencias mencionadas por ambos grupos para la protección de las instalaciones, se concentran alrededor de temas equivalentes, su perspectiva difiere en cuanto al orden de importancia de las mismas. La principal coincidencia es que un gran número de entrevistados (más del 50% de cada grupo), mencionaron recomendaciones relacionadas con la implementación de políticas y control de acceso de personas a las instalaciones de cómputo.

Ver respuestas en la Tabla 8, así como en la Gráfica 6.

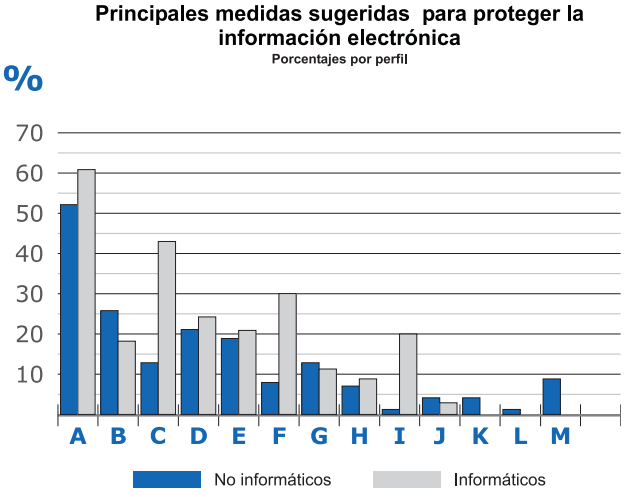
TABLA 8

Principales medidas para proteger las instalaciones físicas (Site)

Tabla de frecuencias

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Políticas / implementación de controles de acceso	439	218	657	52.3%	60.6%	36.6%	18.2%	54.8%
Centro de cómputo cerrado / aislado	217	65	282	25.8%	18.1%	18.1%	5.4%	23.5%
Instalaciones físicas adecuadas	115	155	270	13.7%	43.1%	9.6%	12.9%	22.5%
Supervisión y vigilancia adecuadas	174	87	261	20.7%	24.2%	14.5%	7.3%	21.8%
Sistemas de administración de energía	158	75	233	18.8%	20.8%	13.2%	6.3%	19.4%
Equipo contra incendio	65	108	173	7.7%	30.0%	5.4%	9.0%	14.4%
Contar con proveedores confiables	106	42	148	12.6%	11.7%	8.8%	3.5%	12.3%
Políticas integrales y una cultura de seguridad en inf.	59	30	89	7.0%	8.3%	4.9%	2.5%	7.4%
Medidas de protección civil	8	72	80	1.0%	20.0%	0.7%	6.0%	6.7%
Mantenimiento adecuado de instalaciones	32	10	42	3.8%	2.8%	2.7%	0.8%	3.5%
Reclutamiento y selección de personal adecuados	32	-	32	3.8%	-	2.7%	-	2.7%
Limpieza	8	-	8	1.0%	-	0.7%	-	0.7%
NS/NC	74	-	74	8.8%	-	6.2%	-	6.2%

GRÁFICA 6



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

Después del rubro de políticas y control de acceso, para los "Informáticos" las tres recomendaciones más mencionadas correspondieron a instalaciones físicas adecuadas (aire acondicionado, cableado bien colocado, espacio suficiente, uso de plafón, etc.), equipo contra incendio y medidas de protección civil, mientras para los "No informáticos" fueron tener un Centro de Cómputo aislado, supervisión y vigilancia adecuados (cámaras de video, personal de vigilancia, etc.) y sistemas de administración de energía.

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

Tanto "Informáticos" como "No informáticos" piensan, en una proporción importante de ambos grupos, que la información disponible sobre soluciones de seguridad, es insuficiente. El grupo de los "Informáticos" opina que falta mucha difusión para promover una verdadera conciencia alrededor de la Seguridad en Informática. Este grupo también considera que existe poca difusión sobre productos y soluciones enfocados a las PyMEs y considera que debería darse más énfasis a la capacitación y educación de usuarios.

Ver respuestas en la Tabla 9 y la Gráfica 7.

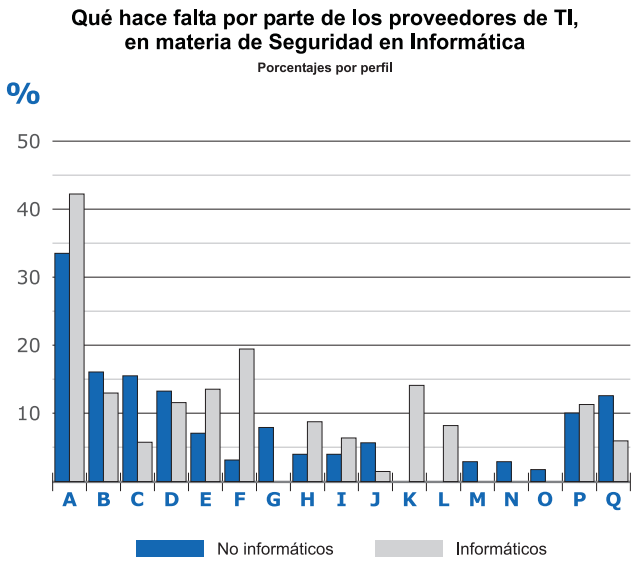
TABLA 9

Qué hace falta por parte de los proveedores de TI en materia de Seguridad en Informática

Tabla de frecuencias

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Información / más difusión	285	152	437	33.9%	42.2%	23.8%	12.7%	36.4%
Mejoras en los procesos de actualización de software	133	47	180	15.8%	13.1%	11.1%	3.9%	15.0%
Mayor asesoría / consultoría	130	21	151	15.5%	5.8%	10.8%	1.8%	12.6%
Políticas razonables de precio	109	42	151	13.0%	11.7%	9.1%	3.5%	12.6%
Capacitación	59	49	108	7.0%	13.6%	4.9%	4.1%	9.0%
Información de soluciones para PyME	25	71	96	3.0%	19.7%	2.1%	5.9%	8.0%
Facilidad de uso de hardware y software	66	-	66	7.9%	-	5.5%	-	5.5%
Mejor integración de productos y soluciones	31	30	61	3.7%	8.3%	2.6%	2.5%	5.1%
Mayor capacidad técnica de los proveedores	32	24	56	3.8%	6.7%	2.7%	2.0%	4.7%
Sistemas de identificación y control de usuarios	45	7	52	5.4%	1.9%	3.8%	0.6%	4.3%
Soluciones ad-hoc para cada empresa	-	51	51	-	14.2%	-	4.3%	4.3%
Más énfasis en el desarrollo de sitios seguros en Internet	-	28	28	-	7.8%	-	2.3%	2.3%
Mejores mecanismos contra piratería	24	-	24	2.9%	-	2.0%	-	2.0%
Mejores soluciones contra hackers	24	-	24	2.9%	-	2.0%	-	2.0%
Garantías comerciales	17	-	17	2.0%	-	1.4%	-	1.4%
Otros	84	42	126	10.0%	11.7%	7.0%	3.5%	10.5%
NS/NC	107	21	128	12.7%	5.8%	8.9%	1.8%	10.7%

GRÁFICA 7



- **A** Información / más difusión
- **B** Mejoras en los procesos de actualización de software
- **C** Mayor asesoría / Consultoría
- **D** Políticas razonables de precio
- **E** Capacitación
- **F** Información de soluciones para PyME
- **G** Facilidad de uso de hardware y software
- **H** Mejor integración de productos y soluciones
- **I** Mayor capacidad técnica de los proveedores
- **J** Sistemas de identificación y control de usuarios
- **K** Soluciones ad-hoc para cada empresa
- **L** Más énfasis en el desarrollo de sitios seguros en Internet
- **M** Mejores mecanismos contra piratería
- **N** Mejores soluciones contra "*hackers*"
- **O** Garantías comerciales
- **P** Otros
- **Q** NS/NC - No-Sabe / No Contestó

Por el lado de los usuarios "No informáticos", piensan que la difusión es escasa respecto de lo que debe hacerse en situaciones consideradas por ellos críticas, como el ataque de virus en una empresa y la posibilidad de que los "hackers" ataquen los sistemas corporativos. Es notorio en este segmento, la percepción de que falta un mayor apoyo de asesoría por parte de los proveedores hacia los usuarios finales, no sólo en relación con los productos que comercializan, sino también en cuanto a políticas generales de seguridad.

Ambos grupos consideran que los mecanismos de actualización de software (antivirus, parches de solución de vulnerabilidades, etc.) deberían mejorarse y ser más oportunos.

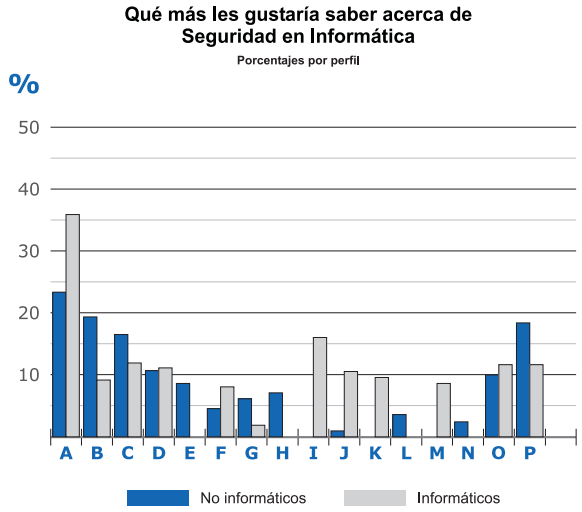
Qué más les gustaría conocer acerca de Seguridad en Informática

Las principales expectativas por conocer algo más relacionado con la Seguridad en Informática, para ambos grupos, corresponden básicamente al control de acceso de usuarios y confidencialidad de la información. Ver las estadísticas de las respuestas en la Tabla 10 y la Gráfica 8.

Tabla 10

Qué más les gustaría saber acerca de Seguridad en Informática
Tabla de frecuencias

	FRECUENCIA (fx)			PORCENTAJES				
	Actividad / Puesto			De su categoría		Del total de respuestas		
	No informáticos	Informáticos	Total	No informáticos	Informáticos	No informáticos	Informáticos	Total
Control de acceso de usuarios, hardware y software	194	129	323	23.1%	35.8%	16.2%	10.8%	26.9%
Más acerca de virus	163	33	196	19.4%	9.2%	13.6%	2.8%	16.3%
Seguridad en Internet	141	43	184	16.8%	11.9%	11.8%	3.6%	15.3%
Más acerca de Hackers	87	40	127	10.4%	11.1%	7.3%	3.3%	10.6%
Seguridad en Informática en general	72	-	72	8.6%	-	6.0%	-	6.0%
Casos de éxito en la materia	36	28	64	4.3%	7.8%	3.0%	2.3%	5.3%
Información de riesgos y soluciones para PyME	54	7	61	6.4%	1.9%	4.5%	0.6%	5.1%
Sistemas de respaldo de información	60	-	60	7.1%	-	5.0%	-	5.0%
Monitoreo y administración de redes	-	58	58	-	16.1%	-	4.8%	4.8%
Manejo general de información	8	38	46	1.0%	10.6%	0.7%	3.2%	3.8%
Costo-Beneficio de los diferentes productos y servicios	-	35	35	-	9.7%	-	2.9%	2.9%
Difusión de los planes de Investigación y Desarrollo	30	-	30	3.6%	-	2.5%	-	2.5%
Seguridad en telecomunicaciones	-	30	30	-	8.3%	-	2.5%	2.5%
Políticas y procedimientos	20	-	20	2.4%	-	1.7%	-	1.7%
Otros	84	42	126	10.0%	11.7%	7.0%	3.5%	10.5%
NS/NC	153	42	195	18.2%	11.7%	12.8%	3.5%	16.3%



Gráfica 8

A Control de acceso de usuarios, hardware y software
B Más acerca de virus
C Seguridad en Internet
D Más acerca de "hackers"
E Seguridad en informática en general
F Casos de éxito en la materia
G Información de riesgos y soluciones para PyME
H Sistemas de respaldo de información
I Monitoreo y administración de redes
J Manejo general de información
K Costo-beneficio de los diferentes productos y servicios
L Difusión de los planes de Investigación y Desarrollo
M Seguridad en telecomunicaciones
N Políticas y procedimientos
O Otros
P NS/NC - No Sabe / No Contestó

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

- Cómo restringir los accesos a su máquina.
- Candados para limitar el acceso a equipos y programas.
- Cómo identificar a las personas que hayan tenido acceso.
- Prevención de ataques de terceras personas.
- Restringir el acceso a archivos.

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

- Seguridad perimetral, en general.
- Firewalls / Proxy.
- Herramientas para disfrazar las direcciones IP que se utilizan.
- Protección de puertos.
- Cómo restringir los accesos a su máquina.

Monitoreo y administración de redes es una inquietud expresada por una proporción importante de los entrevistados "Informáticos", mientras que ningún "No informático" manifestó querer conocer más a este respecto.

Los siguientes tres temas más mencionados por los "No informáticos" se refirieron principalmente a conocer más acerca de virus, seguridad en Internet y más acerca de "*hackers*", mientras que para los "Informáticos" fueron seguridad en Internet, "*hackers*" y manejo general de información.

Percepción acerca de diversas marcas asociadas con Seguridad en Informática

Es notoria una menor identificación (recordación o reconocimiento) de marcas por parte de los No-informáticos, que de los Informáticos. Resultó notorio también, que los No-informáticos suelen asociar, en mucho mayor medida que los Informáticos, el concepto de "seguridad" con marcas de computadoras (PCs).

Las respuestas clasificadas de ambos grupos, pueden consultarse en las respectivas Tabla 11 y Tabla 12.

TABLA 11

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

Marca	Menciones como marca buena (fx)	Menciones como marca deficiente(fx)	Principales Fuerzas	Principales Deficiencias
3Com	30	-	Buen Rendimiento	
Cajas Blancas	-	80	Bajo Precio	Poco Robusto. Poco Servicio.
Cisco	29	-	Marca reconocida	Alto Costo
Compaq	-	13		Bajo Rendimiento
Dell	58	31	Bajo Precio	Poco Servicio
HP	175	-	Marca reconocida	
IBM	29	-	Marca reconocida	
Macintosh	27	-	No compatible (mayor seguridad)	
McAfee	109	46	Bajo Precio. Fácil de actualizar	Poco Soporte
Microsoft en general (MS)	77	86	Marca reconocida	Poca eficacia de las soluciones
MS Windows en general	-	19		Poco Robusto. Inestabilidad
MS-Outlook	-	28		Poco Robusto
Rainbow	10	-	Eficaz	
Roxio	20	-	Marca reconocida (backups)	
Symantec	257	14	Marca reconocida. Buen Soporte. Fácil de actualizar	Poca eficacia de las soluciones
Toshiba	19	-	Marca reconocida (laptops)	
VeriSign	21	-	Marca reconocida. Especialización Financiera	
Otros	107	105		
NS/NC	219	503		

TABLA 12

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

Marca	Menciones como marca buena (fx)	Menciones como marca deficiente(fx)	Principales Fuerzas	Principales Deficiencias
3Com	58	-	Buena tecnología	Poca presencia de marca
Avaya	21	-	Buena estrategia de implementación	
CA Innoculate	12	-	Soluciones integrales	Poca eficacia de soluciones
Checkpoint	40	-	Buenos para Internet	
Cisco	91	-	Líder en el mercado	Altos costo de implementación
Dell	26	-	Bajo costo	
IBM	-	25		Falta de atención a elementos de seguridad
Java	27	-	Versátil	
Linux	56	-	Mucho control para el usuario. Flexible	No Marca reconocida
McAfee	87	51	Altamente confiable	Poco soporte
Microsoft en General (MS)	17	43	Marca reconocida	Poco Confiable
MS Windows 2000	39	-	Mucho control para el usuario	
MS Windows en General	-	75	Marca reconocida	Poco Confiable
MS Windows NT	20	-	Marca reconocida	
MS Windows diferentes a NT	-	31	Marca reconocida	Poco Confiable
MS-SQL	25	-	Flexible	Poco Soporte
Oracle	28	-	Robusto	Alto Costo. Poco Flexible. Poco Soporte
OSX (Apple)	21	-	Flexible	Poco Confiable
Rainbow	15	-	Robusto	
Sonicwall	33	-	Robusto	
SSL	19	-	Marca reconocida	
Sun-Solaris	41	-	Robusto	No Marca reconocida
Symantec	142	-	Robusto. Buen Soporte	Poco Robusto. Poca eficacia de soluciones
Tarjetas Genéricas	-	17		Bajo rendimiento
Trend Micro	14	-	Bajo costo	Poco Robusto
VeriSign	30	-	Marca reconocida. Especialistas en seguridad	Alto costo
WatchGuard	29	-	Difícil implementación	
Wingate	14	-	Bajo Costo	Poco Robusto
Otros	15	84		
NS/NC	12	107		

III. Estudio con proveedores líderes del mercado de TI

Objetivos del estudio

1. Conocer la percepción que proveedores cuyas soluciones tienen incidencia 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 proveedores líderes de soluciones informáticas que operan en México, respecto del mercado actual de Seguridad en Informática, y compilar las diferentes visiones que tienen en cuanto a su desarrollo.

Metodología

Método de investigación

El estudio se realizó a través de cuestionario estructurado

Relación de entrevistados

Si bien la mayoría de los entrevistados estuvo de acuerdo en que se les mencionara como participantes en este estudio, tanto a nivel personal como de empresa, dos de ellos solicitaron confidencialidad en cuanto a su identidad. Cabe mencionar, sin embargo, que sus opiniones están incluidas en este análisis, ya que la posición de sus organizaciones como empresas líderes en su ramo (tanto nacional como internacionalmente), son de gran valor para la industria y para todos los interesados en la Seguridad en Informática de nuestro país.

Empresa	Nombre	Puesto
3Com	Ignacio Leñero	Director General
Advantage Security Systems	John Gregory	Gerente General
Asiste	Moisés Polishuk	Director General
Confidencial	Confidencial	Confidencial
Confidencial	Confidencial	Confidencial
Digital Video Box	Axel Vera	Director General
EDS	Germán Arena	Gerente de seguridad de la Información L.A. Norte.
Grupo Vilsa	Luis Raúl Vidales	Director General
Iron Mountain	Guillermo Guerra	Director General
ITESM	Francisco Camargo	Director de Informática
Kio Networks	José Fonseca	Director General de Outsourcing
Mexel-Dominion	Arturo Vázquez	Gerente de Ventas-Distribución
Microsoft México	Eduardo Pierdant	Gerente de Mercadotecnia en Seguridad Informática

Opentec	Carl Rianhard	Presidente
Oracle México	Javier Cordero	Director General
Rainbow Technologies México	René Cobián	Gerente de Seguridad y desarrollo de Canal para México y La Región Andina
Sinapsis	Alejandro Rodríguez	Director de Marketing y Nuevos Negocios
Sun Microsystems	Jaime Vallés	Director General
Symantec	Gabriel Alvarado	Director General México, Centro América, Caribe y Chile
Telesma	David Cárdenas	Director General

Resultados

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

En general, se percibe cierto rezago en nuestro país, considerando su nivel entre medio y bajo frente a los países más industrializados del mundo. Se habló de diferentes causas posibles, relacionadas, principalmente, con una baja promoción de la cultura de seguridad en general y una pobre asignación de recursos a este rubro, por parte de las organizaciones, sobre todo en las de infraestructura mediana y pequeña.

Principales observaciones

Salvo empresas de clase mundial, existen deficiencias en la planeación e instrumentación de políticas de Seguridad en Informática.

A pesar del rezago (de 1.5 años respecto de Estados Unidos, aproximadamente), México está acelerando cada vez más su avance en la materia.

El nivel de conciencia respecto de la Seguridad en Informática, en general, se considera bajo. Sobresalieron las siguientes apreciaciones:

- Hay menor conciencia en la PyME, que en los grandes corporativos.
- Existe una mayor conciencia entre los niveles técnicos, que entre los niveles ejecutivos.
- A nivel de jerarquía organizacional, se considera que mientras más alto es el nivel, existe una mayor conciencia.

Falta entendimiento de Seguridad en Informática. Debe ser vista como parte de toma de decisión de negocio y no como un proceso tecnológico. Se está más enfocado a herramientas que a cuestiones estratégicas. Y aún así, las herramientas utilizadas suelen ser muy básicas.

La situación económica del país y de las empresas en general, provocan que se destinen pocos recursos al rubro de Seguridad en Informática.

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

Las respuestas codificadas de todos los entrevistados (quienes dieron, en la mayoría de los casos, más de una opinión cada uno), giraron alrededor de 5 rubros principalmente, como puede observarse en la Gráfica 9.

GRÁFICA 9

PRINCIPALES OBSERVACIONES

Hay coincidencia en que falta una difusión generalizada, tanto desde el punto de vista didáctico y de desarrollo profesional, como a nivel informativo.

Se perciben huecos legales e inestabilidad jurídica respecto de diversos aspectos relacionados con la Seguridad en Informática, como son el hecho que la tecnología avanza mucho más rápido que el proceso de creación de leyes, la diversas instancias en las cuales se puede tener o no certeza jurídica de la validez de un documento electrónico, la forma legal de determinar el daño que un pérdida electrónica puede tener para una persona u organización, y, en general, la falta de un marco jurídico sólido respecto de aspectos electrónicos.

En cuanto a la Cultura de Seguridad Integral, se mencionó que todo esfuerzo por configurarla debe contemplar varios rubros. La capacitación no debe limitarse a nociones básicas de seguridad para las PCs. El tema de la Seguridad en Informática debería estar relacionado con el tema del ciclo de vida de la información y abarcar, desde el momento en que ésta se genera, hasta su resguardo para fines legales, contables u operativos.

En cuanto a la asignación de recursos para este rubro, se menciona el financiamiento como una necesidad indispensable para que los fabricantes sigan teniendo clientes y para que las empresas y organizaciones puedan contar con los beneficios de la tecnología en este sentido.

Entre otros retos de importancia, se mencionaron:

- Lograr un comercio electrónico cien por ciento seguro.
- Definir, por un lado, y difundir por el otro, estándares concretos de seguridad.
- Definición de arquitecturas adecuadas y soluciones integrales.
- Uso generalizado de herramientas de seguridad en todo el país.
- Establecimiento de bases y políticas. Mayor planeación.
- Mejores procesos de administración interna en las empresas y mayor apertura hacia alternativas de software.
- Promover la conciencia de la Seguridad en Informática, a nivel de individuo.
- Protección de la propiedad intelectual.

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

De acuerdo a las principales opiniones de los entrevistados, los retos que las empresas e instituciones usuarias de la tecnología tienen en primer orden, es el de concientizar a los directivos en materia de Seguridad en Informática y capacitar a sus empleados, así como establecer bases correctas y políticas claras. Se piensa que la gran mayoría de las organizaciones del país, no se han dado cuenta que invertir en Seguridad en TI es una necesidad y no un lujo.

Principales observaciones

Aparte de políticas, hace falta implementar metodologías a nivel interno.

Es importante que las empresas incorporen estándares de nivel internacional, lo exijan así a sus proveedores y cuenten con personal suficientemente especializado.

El desarrollo de sistemas en sí mismo y su implementación interna, es un reto que la empresa debe solventar.

Los procesos y procedimientos de Seguridad en Informática dentro de las empresas, deben ser continuamente revisados y actualizados, como parte de sus programas o políticas internas.

Entre otros retos de importancia, se mencionaron:

- Promover una mayor conciencia entre los niveles directivos de la empresa, respecto de las posibles vulnerabilidades y las implicaciones de no tener una infraestructura primaria segura. Es un tema que no debe delegarse totalmente a las áreas de Sistemas.
- Realmente implementar y no sólo quedarse en el plan.
- Asignar mayores recursos a la Seguridad en Informática, haciendo una inversión inteligente.
- Promover y exigir una legislación adecuada.
- Simplificar el modelo de aplicación de la seguridad de la información.

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

Hablando específicamente de fabricantes de equipos, uno de los principales retos percibidos es que se incluyan más mecanismos de seguridad en ellos y que no dejen toda la responsabilidad a los fabricantes de software. En este sentido, es importante que no reduzcan funciones de seguridad con tal de bajar sus precios; su competencia frente a otras marcas, debería ser no sólo en cuanto a precio, sino en los valores agregados que podrían existir alrededor de tecnología cada vez más segura.

Una oportunidad para la industria, en la cual se incluyen ventajas para los usuarios, es percibida en la integración de "bundles" de productos o herramientas de Seguridad en Informática, en la oferta de los equipos.

Destaca un alto número de menciones que sugieren que la producción de hardware de diferentes marcas, debe estar enfocada a facilitar la integración en ambientes heterogéneos o bien a la estandarización de soluciones.

Asimismo, existe coincidencia en cuanto a que debería haber una mayor oferta de productos específicos para Seguridad en Informática.

Principales observaciones

La creación de una Cultura de Seguridad en Informática integral, también se considera una responsabilidad de este sector.

Deben dimensionar adecuadamente sus productos para la venta al cliente, buscando el mejor balance costo-beneficio. Crear una oferta con buen retorno sobre la inversión.

Entre otros retos de importancia, se mencionaron:

- Creación de soluciones más globales.
- Que sepan hacer las recomendaciones óptimas de seguridad para sus productos.
- Diseñar herramientas con mayor tolerancia a fallas, con mejores precios.
- Impulsar más la investigación para el desarrollo tecnológico.
- Enfocar soluciones a la administración centralizada.
- Producir equipos que a través de firmware pueda irse actualizando a medida que se conoce alguna vulnerabilidad.
- Olvidarse de una vez por todas, de la venta de cajas.

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

De manera similar a lo comentado respecto de los fabricantes de hardware, uno de los principales retos de los proveedores de software es el poder facilitar la integración de soluciones en ambientes heterogéneos. Ésta es una exigencia tanto de usuarios como de integradores, en donde ambas industrias tienen que buscar coincidencias y desarrollar sus productos bajo esta perspectiva.

En particular, los fabricantes de software deben incrementar las funciones de seguridad en sus productos, sin escatimar ningún aspecto por bajar precios, eliminando al máximo las vulnerabilidades.

Se menciona también la formación de "bundles" de productos de seguridad, como una estrategia comercial adecuada.

Un punto a destacar, es que los fabricantes de software deberían desarrollar aplicaciones con mayor capacidad de registro de actividades.

Principales observaciones

Al igual que los proveedores de hardware, se considera que los fabricantes de software deben compartir la responsabilidad de crear una mayor cultura de seguridad en informática, buscar el desarrollo de aplicaciones más estandarizadas, bajo especificaciones globales, promover soluciones con administración centralizada, mayores recursos para investigación y desarrollo, e incremento de su oferta de productos relacionados con la seguridad en informática, entre otros.

Algunos de los retos específicos que fueron mencionados, son:

- Mayor oportunidad en la producción y liberación de actualizaciones , relacionadas con seguridad.
- Ampliar el ciclo de vida de los productos, para que sean seguros. Tenerlos perfectamente probados y fortalecidos, en vez de estar liberando "betas" todo el tiempo.
- Desarrollar aplicaciones que por sí mismas, sean más resistentes a virus.
- Difundir información de manera inmediata cuando se detecten fallas.
- Mantener el balance adecuado entre la calidad aplicativa y los controles de calidad de los códigos.
- Evitar el desarrollo de aplicaciones que pretendan hacer todo.
- Que el software cuente con políticas de seguridad dentro de sí mismo.
- Ofrecer soluciones con un buen retorno sobre la inversión.
- Utilizar lenguajes seguros de programación, buscar alternativas y sistemas operativos seguros.

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

En opinión de los entrevistados, desde el punto de vista del integrador la Seguridad en Informática debe ser parte de la solución y no un valor agregado. Debe estar implícita en cualquier propuesta tecnológica.

Uno de los retos mencionados con mayor frecuencia, es que los integradores deben contar con expertos en seguridad y estar mejor capacitados en cuanto a los alcances y especificaciones de los productos que utilizan. Asimismo, deben conocer mucho más al cliente y su entorno de negocios, con una sólida especialización en mercados verticales para ofrecerles las soluciones con el mejor balance costo-beneficio.

Principales observaciones

Entre otros retos de importancia, se mencionaron:

- Crear una visión integral de seguridad, educar a sus clientes y promover el valor de la seguridad entre ellos.
- Agrupar correctamente los elementos de hardware, software y servicios
- Tener una adecuada definición y cumplimiento de metodologías.
- Incorporar a sus servicios / propuestas, soluciones con robustez, confiabilidad y control.
- Ofrecer asesoría inteligente y servicios diferenciados de Alto Valor, como auditorías, etc.
- Integrar a su oferta, servicios de aseguramiento de redes y computadoras.
- Vender una Cultura de Seguridad, no hardware.

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

Entre lo más importante, se considera que las instituciones educativas deben preparar y desarrollar verdaderos profesionales en el campo de la Seguridad en Informática, e incluso incorporar un mayor número de carreras y materias especializadas.

La Seguridad en Informática debe ser una parte relevante dentro de sus programas educativos, no sólo en materias afines a la tecnología, sino también en carreras y capacitaciones de otros ramos, en donde existen futuros o actuales ejecutivos.

Como corresponde a su actividad, se considera que estas organizaciones deberían ser de las principales promotoras de una Cultura de Seguridad en Informática en todos los niveles, así como uno de los agentes más importantes para la creación de conciencia en la materia.

Principales observaciones

Entre otros retos de importancia, se mencionaron:

- Promover valores de ética y responsabilidad.
- Mantener una postura neutral respecto de software libre y propietario. No polarizar a los estudiantes en este sentido.
- Promover argumentos para invertir en soluciones de seguridad y desarrollo de herramientas ROI.
- Instruir a los alumnos en el uso correcto de Internet y el correo electrónico.
- Realizar estudios para evaluar las consecuencias sociales y económicas a futuro.
- Aumentar la cantidad de carreras y cursos virtuales.
- Implementar soluciones de seguridad en sus propios sistemas.

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

La función educativa de los medios, fue mencionada de manera consistente. En general, se considera que deben concienciar y educar con responsabilidad a las personas en el uso de herramientas electrónicas.

Asimismo, se considera que los medios deben tomar más en serio el tema de Seguridad en Informática y ligar las noticias relacionadas a eventos de la vida diaria, evitando caer en amarillismos.

Principales observaciones

Entre otros retos y sugerencias a los medios de comunicación, se mencionaron:

- Entender los problemas y estar actualizados para informar correctamente al público, a través de consultar a expertos con juicios confiables para analizar las noticias de seguridad en informática.
- Informar acerca de problemas, beneficios de la seguridad en informática, empresas que tengan soluciones y casos de éxito.
- Apoyar la desmitificación de la complejidad de la informática.
- Fomentar, generar y ganar la confianza de los usuarios para el uso masivo del comercio electrónico.
- Mayor difusión de riesgos.
- Enfocar programas para educar a los niveles ejecutivos de las organizaciones.
- Emitir noticias sin sesgos hacia marcas de productos.
- Mayor presencia de temas relacionados con la Seguridad en Informática en las secciones de Negocios de los medios.
- Crear un canal especializado en TI, al cual se incorpore después una sección dedicada a la Seguridad en Informática.

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

Prácticamente la mitad de los entrevistados coincidieron, de manera espontánea, en que existen carencias en materia de Reglamentación y Regulación, normas y leyes sobre la electrónica que contemplen sanciones apropiadas. En este rubro es donde el gobierno tendría su mayor reto, según sus respuestas.

Asimismo, el combate a la ignorancia y la difusión de una cultura en materia de Seguridad en Informática a la ciudadanía, son consideradas como prioridades.

Principales observaciones

Entre otros retos, se mencionaron:

- Difusión de riesgos.
- Entender el entorno, difundir la información, y promover la implementación de soluciones.
- Impulsar un gobierno digital.
- Crear y establecer políticas de fomento informático a nivel nacional (PYMEs).
- Promover programas de financiamiento para PYMEs.
- Integrar más procesos electrónicos para la ciudadanía, como usuario de sus servicios.
- Protección adecuada de sus sistemas de acceso al público en general.
- Mayor inversión en investigación y desarrollo de sistemas de Seguridad en Informática.
- Mayor exigencia en el cumplimiento de estándares.
- Empezar en casa, implementando soluciones seguras que realmente funcionen.
- Crear o adoptar estándares que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Contar con especialistas para investigación y fallos adecuados en Seguridad en Informática.
- Evitar el uso de aplicaciones que usen modelos propietarios.

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

3Com

Ignacio Leñero / Director General

"En 3Com estamos desarrollando Hardware y software de seguridad para organizaciones de cualquier tamaño, de tal manera que podemos garantizar el acceso a la red de voz y datos a personas autorizadas, así como protegerla de intrusos, de contenidos no deseados, protección a las estaciones de trabajo y a los servidores".

Advantage Security Systems

John Gregory / Gerente General

"Oferta de soluciones en todos los sectores de seguridad de informática, experiencia extensiva, personal certificado y altamente calificado".

Asiste

Moisés Polishuk / Director General

"Evolucionando a aplicar correctamente la tecnología para seguridad en los negocios".

Digital Video Box

Axel Vera / Director General

"Instalando sistemas de protección tipo firewalls en todos nuestros sistemas, y educando a los usuarios para su correcta utilización".

EDS

Germán Arena / Gerente de Seguridad de la Información L.A. Norte

"EDS cuenta con Grupo a Nivel Mundial dedicado a la Seguridad de la Información, cubriendo las principales infraestructuras de sistemas (Mainframe, AS400, Unix, Microsoft y Linux) y comunicaciones.

"Brindando servicios que permiten:

- *Identificar el Nivel de Seguridad existente.*
- *Diseñar la Arquitectura de Sistemas y Comunicaciones más adecuada.*
- *Desarrollar Políticas y Procedimientos de Seguridad que se apeguen a las necesidades del Negocio.*
- *Implementación de la Infraestructura de Seguridad.*
- *Administración (Outsourcing) de la Infraestructura de Seguridad".*

Iron Mountain

Guillermo Guerra / Director General

"En Iron Mountain, protegemos y administramos los medios magnéticos de las empresas, al tiempo que custodiamos su información:

1. *"Off-Line (fuera de línea): para mayor seguridad frente a agresores externos, como hackers, virus, etc.*
2. *"Off-Site: para mayor seguridad física de su información, y para garantizar la recuperación rápida de su información en caso de desastre*
3. *"Out-of-reach (fuera de alcance): para mayor seguridad contra agresores internos, como sabotajes".*

ITESM

Francisco Camargo / Director de Informática

"El Tecnológico de Monterrey ha hecho tres grandes aportaciones:

1. *"Desde 1998 tienen un departamento de seguridad en informática. Todas las carreras y maestrías en sistemas, así como las MBA's, llevan temas de seguridad en informática.*
2. *"En conjunto con la ALAPSI, tienen un diplomado en seguridad computacional.*

3. *"Promoción en la comunidad del campus, bajo el nombre de "campus seguro", de conceptos de seguridad en informática para alumnos, maestros y padres de familia".*

Kio Networks

José Fonseca / Director General de Outsourcing

"Nuestra empresa maneja un modelo integral único de seguridad que resuelve varios aspectos críticos:

- *"Seguridad fisica, al tratarse del centro de datos de altas especificaciones con niveles de seguridad fisica únicos en México y Latinoamérica.*
- *"Seguridad lógica, al contar con servicios integrales de seguridad que van desde la definición de políticas corporativas de seguridad, la integración de soluciones de alta disponibilidad y seguridad en cualquier plataforma y tecnología, la operación, monitoreo y detección automática de intrusos, accesos no autorizados e intentos de violación, de manera continua las 24 horas del día los 365 días del año, por medio de herramientas de última tecnología.*
- *"Recuperación de desastres y continuidad de negocios, al ser una corporación de servicios de tecnología de información, que pone a disposición de sus clientes espacios de oficina (business park) y centro de datos de altas especificaciones, aparejados a los servicios profesionales para el desarrollo de sus planes de recuperación y continuidad, habilitación de la infraestructura necesaria y operación de contingencia a cualquier grado de sofisticación y cualquier tiempo de recuperación requerido".*

Mexel – Dominion

Arturo Vázquez / Gerente de Ventas – Distribución

- *"Soluciones de seguridad basadas en estándares (Ipsec, 3DES,...).*
- *"Servicios de auditorías en vulnerabilidad informática para PYMES.*
- *"Soluciones llave en mano completas (antivirus, firewalls, incriptores, balanceadores IP, administradores de ancho de banda L1-L7. etc).*
- *"Implementar las soluciones a nivel de consultoría, guiar al cliente por la mejor solución que requiera. Adicionalmente, implementar esquemas más robustos de autenticación y autorización para proteger sus recursos.*
- *"Establecer relaciones a largo plazo con nuestros clientes y proveedores (Mexel-Dominion cumplimos 34 años el 12 de Oct/04, en el campo de instrumentación e informática en México)".*

Microsoft México

Eduardo Pierdant / Gerente de Mercadotecnia en Seguridad Informática

"Atacando los 3 grandes retos mencionados:

1. *"Haciendo uso de medios de comunicación masiva, Internet, etc. Comunicar las acciones que un usuario debería realizar para mantener su PC segura. Artículos en revistas de alta divulgación para usuario final sobre "buenas prácticas y costumbres" en el uso de la computadora e Internet*
2. *"Dentro de los eventos de la compañía, las interacciones con nuestros clientes, las llamadas realizadas, incluir el mensaje de qué debe hacerse para mantener los activos informáticos de las compañías seguras.*
3. *"Seminarios de entrenamiento gratuito para todos los ingenieros y profesionales de las tecnologías de información, a partir del mes de Marzo, en más de quince (15) ciudades de la República Mexicana".*

Opentec

Carl Rianhard / Presidente

"Todas nuestras líneas de negocios están enfocadas hacia la seguridad de las redes y la información asociada. Somos un Partner de Symantec e implementamos soluciones integrales de seguridad.

"Opentec es un proveedor de soluciones de CRM y mesas de ayuda, donde damos soporte a nuestros clientes con la administración de sus propios clientes. Esto requiere de un manejo estricto de bases de datos, integridad de los servidores, dimensionamiento del ancho de banda, etc. Nuestros clientes tienen que confiar en que sus clientes serán protegidos al 100%.

"Por ultimo, Opentec es líder en soluciones de E-learning y educación a distancia. Estamos en la era del conocimiento en el cual el activo más importante que tienen las empresas es su gente y el conocimiento que cada persona aplica en su trabajo diario. Opentec maneja información muy confidencial de estrategias de negocios, códigos de ética, precios y promociones, todo esto vía Internet, en forma de educación a distancia, con miles de usuarios en diversos países. Imagínense que la competencia de algún cliente pudiera tener acceso a esta información confidencial. La integridad de la información comienza con un Servidor Opentec robusto, sistema operativo de Microsoft seguro, base de datos SQL de Microsoft, también protegido, un sistema de conocimiento propio llamado Mentor y el contenido del cliente integrado, con accesos y claves sobre un sitio seguro.

"Opentec maneja la integridad absoluta de la información de nuestros clientes con una combinación de hardware y software de clase mundial y con políticas de uso que aseguran un buen funcionamiento".

Oracle México

Javier Cordero / Director General

"Oracle es hoy el único software de manejo de Base de Datos que cumple con 17 de los estándares definidos a nivel internacional.

"Además, ofrece la facilidad de implementar elementos adicionales como encripción de datos, seguridad por roles y algunas otras características que permiten incrementar los niveles de seguridad en aplicaciones hechas en casa".

Rainbow Technologies México

René Cobián / Gerente de Seguridad y Desarrollo de Canal para México y la Región Andina

"Somos un activo promotor de la cultura en seguridad informática. Nuestro portafolios incluye soluciones para aspectos claves en ese sentido: autenticación, encripción, VPN´s seguras y PKI".

Sinapsis

Alejandro Rodríguez / Director de Marketing y Nuevos Negocios

"Trece años vendiendo seguridad, con inversión fuerte en estructuras seguras".

Sun Microsystems

Jaime Vallés / Director General

"Todos los sistemas operativos que comercializamos son altamente seguros, tanto Solaris como JDS (basado en Linux). De la misma forma tenemos prácticas de consultoría sobre seguridad, cómo implementarla y cómo mantenerla".

Symantec

Gabriel Alvarado / Director General México, Centroamérica, Caribe y Chile

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

"Symantec cree firmemente que la visión de la seguridad consta de procesos preventivos o de alerta temprana, reactivos o de protección, de respuesta y de administración, que en conjunto con planes de difusión de la cultura de seguridad, servicios educativos y procesos de consultoría, administración y monitoreo remoto, permiten a los usuarios de nuestros servicios entender la seguridad como parte de una decisión organizacional no tecnológica, brindándoles la oportunidad de focalizar sus esfuerzos humanos en los objetivos principales de su negocio, descansando la seguridad en una empresa que se considera un socio de negocios de nuestros clientes.

"Symantec ha invertido muchos años en el desarrollo de soluciones contra las amenazas a la seguridad en constante evolución. Comprendemos los retos de seguridad a los que se enfrentan las empresas y los usuarios particulares. Nuestro planteamiento completo para contener las

amenazas, representa el siguiente paso en el desarrollo de soluciones de seguridad más eficaces.

"Asimismo, formamos parte de las organizaciones que buscan fomentar la conciencia de seguridad informática en el país, participando activamente como coordinadores de mesas de trabajo dentro del grupo de Delitos Cibernéticos de la PFP en México; por otro lado, Symantec es considerado líder de opinión en diferentes medios de comunicación para los temas de seguridad informática.

"Hoy Symantec en México apoya y soporta la seguridad de las principales organizaciones en el país, lo que confirma la confianza que nuestra compañía brinda a nuestros usuarios asegurando el éxito en su administración de riesgos".

Ver estrategia de seguridad de Symantec en la Gráfica 10.

Estrategia de seguridad de Symantec

GRÁFICA 10

Grupo Vilsa

Luis Raúl Vidales / DIRECTOR GENERAL

"Vilsa ha participado en los últimos años en fortalecer la imagen de México como un país en donde la seguridad es viable, no sólo en informática sino en cuestiones físicas, colaborando en la seguridad de las diferentes cumbres internacionales celebradas en nuestro país, como por ejemplo: APEC OMC ALCUE, entre otras. En total, apoyando a más de 148 jefes de gobierno y a sus comitivas, en más de siete diferentes cumbres.

"Grupo Vilsa efectúa análisis de riesgo, control de acceso, reconocimiento facial y planeación con la técnica de mind-mapping, que ha permitido integrar soluciones y enfrentar con éxito situaciones de alto riesgo".

Telesma

David Cárdenas / DIRECTOR GENERAL

"Apoyando la educación a ejecutivos con el mensaje correcto".

IV. Conclusiones de la investigación

Panorama general

Los resultados de este estudio permiten observar cuál es la percepción que se tiene acerca de la Seguridad en Informática en las ciudades más importantes de México, desde las diferentes perspectivas que en conjunto nos acercan a la visión general del país en un momento dado. Son un intento planeado y estructurado, por contar con una fotografía del sentir y del conocer de las personas de México, respecto de los conceptos y prácticas de Seguridad durante el primer semestre de 2004.

En primera instancia, son notorias diversas carencias y deficiencias en difusión, capacitación y fomento a la cultura de seguridad en informática, tanto a nivel organizacional como individual, que colocan a México como un país rezagado en la materia y lo ponen en evidente desventaja frente a las vulnerabilidades actuales y latentes. La mayoría de las preocupaciones giran alrededor de los "temibles" virus y "hackers", dejando a un lado o dando menor importancia a otro tipo de riesgos, como pudieran ser una planeación deficiente, escasa o nula, la falta de políticas internas claras y comunicadas adecuadamente, la falta de educación, la negligencia y la inexperiencia, las plagas, los desastres naturales y otro tipo de contingencias, e incluso otros de difícil cuantificación como el brindar un mal servicio y la pérdida de credibilidad y confianza por parte de los clientes, por ejemplo.

Y aún en el caso de los "hackers", tan mencionados durante la encuesta entre usuarios, es poco el conocimiento que se tiene respecto de los efectos que sus acciones pueden tener sobre cualquier tipo de empresa o institución (es un concepto muy mencionado, aunque más esotérico que palpable) y, por consiguiente, no conocen las medidas existentes para contrarrestarlos.

Este desconocimiento acerca de soluciones de Seguridad en Informática, es generalizado entre los niveles medios de las organizaciones (principalmente PyMEs), salvo algunas excepciones entre cierto personal de alta especialización y en los grandes corporativos. En general, se percibe que la Seguridad en Informática, hasta el momento, aún no forma parte importante de la cultura organizacional.

La necesidad de una mayor capacitación, sin embargo, es percibida por una gran cantidad de personas, tanto por quienes consideran que sus subalternos requieren profundizar en el tema, como por los mismos usuarios (informáticos y no informáticos) a quienes les gustaría aprender más acerca de cómo enfrentar los riesgos que amenazan la integridad y la seguridad de la información, así como la confidencialidad de la misma. En este sentido, se percibe una conciencia general de que es necesario conocer más sobre seguridad en informática, y resulta notorio que existe disposición para obtener este conocimiento.

Coincidencias y diferencias entre el usuario "informático" y el "no-informático"

Aunque la percepción de ambos grupos tiende a ser distinta como consecuencia del grado de especialización en materia de informática y telecomunicaciones, existen algunas coincidencias que, entre otras cosas, denotan el comportamiento que se ha dado en la industria, en los medios, en las organizaciones y de boca en boca, por difundir ciertos temas específicos. Entre las principales coincidencias, se mencionan:

- Ambos dan una prioridad similar al respaldo de información, como concepto distintivo de la seguridad en informática.
- Los virus representan la amenaza de mayor riesgo para ambos grupos, seguido de "hackers" y otros agresores externos.
- Los dos grupos perciben el "desconocimiento" como uno de los mayores riesgos contra la seguridad.

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

Usuarios informáticos

- Perciben más la integridad y confiabilidad de la información, como un elemento importante de la seguridad en informática.
- Este grupo tiene mayor conciencia acerca de los daños que podrían ocasionar los agresores internos.
- Mayor preocupación por herramientas de monitoreo y administración.
- Muestran mayor preocupación por contar con instalaciones físicas adecuadas, así como equipos contra incendio, como medida de protección de las instalaciones donde se encuentran los equipos de cómputo y telecomunicaciones.

Usuarios "No-informáticos"

- Se preocupan más por los conceptos de acceso y confidencialidad de la información, y por los ataques de virus.
- Aunque con una frecuencia baja, sólo este grupo hizo menciones que asocian el uso de software original con el concepto de seguridad.
- Poco conocimiento sobre soluciones tecnológicas específicas y un nivel muy bajo de identificación de marcas relacionadas con productos o servicios de seguridad en informática.
- Una mayor proporción de este grupo, recomienda incrementar la capacitación y el uso de contraseñas, como solución ante posibles riesgos.
- Para la protección de instalaciones, los "no-informáticos" mencionaron en mayor proporción que los "informáticos" conceptos como el aislamiento del centro de cómputo, así como una supervisión y vigilancia adecuados.

Principales demandas por parte de los usuarios

Usuarios Informáticos

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

- Información / más difusión
- Información de soluciones para PyME
- Soluciones ad-hoc para cada empresa
- Capacitación
- Mejoras en los procesos de actualización de software
- Políticas razonables de precio

En cuanto a las necesidades más importantes de capacitación y difusión para este grupo de usuarios, se mencionaron las siguientes:

- Control de acceso de usuarios, hardware y software
- Monitoreo y administración de redes
- Seguridad en Internet
- Más acerca de "*hackers*"
- Manejo general de información
- Costo-Beneficio de los diferentes productos y servicios
- Más acerca de virus
- Seguridad en telecomunicaciones

Usuarios "No-informáticos"

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

- Mayor información
- Mejoras en los procesos de actualización de software
- Mayor asesoría / consultoría
- Políticas razonables de precio
- Facilidad en el uso de hardware y software
- Mayor capacitación

Las inquietudes principales de este grupo por aprender y profundizar en el tema de seguridad, giraron alrededor de conceptos como:

- Control de acceso de usuarios, hardware y software
- Más acerca de virus
- Seguridad en Internet
- Más acerca de "*hackers*"
- Seguridad en Informática en general

Principales retos de las entidades organizadas de México

Lo que presentamos en esta sección de Conclusiones, se refiere a los retos que fueron mencionados con mayor frecuencia o cuya relevancia merece que el concepto sea resaltado.

Entidad	Principales retos
Organizaciones usuarias	• Concientización de los niveles directivos, respecto de la necesidad de implementar la seguridad en informática en las organizaciones. • Capacitación de sus empleados. • Establecimiento de políticas claras y estándares de nivel mundial. • Destinar los recursos adecuados a este rubro.
Proveedores de hardware	• Incorporar aspectos de seguridad en sus equipos, como ventaja competitiva y no sólo basarla en precio. • Estandarizar y/o facilitar la integración en ambientes heterogéneos. • Mayor impulso a la investigación y desarrollo, e incremento de su oferta de productos enfocados a la Seguridad en Informática. • Crear soluciones más globales. • Cambiar su esquema tradicional de "comercialización de cajas".
Proveedores de software	• Facilitar la integración de soluciones, sin escatimar recursos. • Promover soluciones con administración centralizada.

	• Mayor oportunidad en la producción y liberación de actualizaciones, relacionadas con seguridad. • Ampliar el ciclo de vida y periodo de prueba de los productos, para que sean seguros. • Difundir información de manera inmediata cuando se detecten fallas.
Integradores de soluciones	• Incorporar la Seguridad en Informática como parte de las soluciones y no como un valor agregado. • Dar mucho énfasis a la capacitación del personal a cargo de proyectos, respecto de los productos que recomiendan o representan. • Conocimiento profundo del cliente y de su entorno de negocios. • Mayor educación y capacitación a sus clientes, promoviendo el valor de la seguridad entre ellos. • Vender una Cultura de Seguridad, no hardware.
Instituciones educativas	• Mayor especialización sobre seguridad, tanto en sus docentes como en sus programas de enseñanza. • Promoción de una Cultura de Seguridad en Informática en todos los niveles. • Promover los valores de ética y responsabilidad. • Ser imparciales respecto del uso de software libre y propietario. • Instruir a sus alumnos en el uso correcto de Internet y del correo electrónico.
Medios de comunicación	• Concientizar y educar con responsabilidad a las personas en el uso de herramientas electrónicas. • Mayor precisión en la difusión de noticias relacionadas con seguridad en informática. • Incorporar a especialistas, al momento de emitir juicios alrededor de temas relacionados. • Difusión de los beneficios de contar con una cultura sólida sobre seguridad en informática a nivel organizacional. • No mitificar ni crear temor alrededor del comercio electrónico. • Mayor difusión de temas relacionados con la Seguridad en Informática, en las secciones de Negocios de los medios.
Gobierno	• Mayor énfasis en materia de Reglamentación y Regulación. Normas y leyes sobre la electrónica, que contemplen sanciones apropiadas. • Refuerzo en el combate a la ignorancia sobre la materia. Mayor difusión de una cultura de Seguridad en Informática. • Impulsar un gobierno digital. • Crear y establecer políticas de fomento informático a nivel nacional. • Promover programas de financiamiento para PYMEs. • Integrar más procesos electrónicos para la ciudadanía, como usuario de sus servicios. • Protección adecuada de sus sistemas de acceso al público en general. • Mayor exigencia en el cumplimiento de estándares.

Áreas de oportunidad para la industria TI

1. La necesidad reconocida por los usuarios de diversos niveles, de contar con mayores conocimientos relacionados con la Seguridad en Informática, permite inferir posibles áreas de oportunidad en diversos rubros y mercados.

    a. **Difusión**. La difusión de temas sobre Seguridad en Informática, puede ser un área de oportunidad tanto para organizaciones especializadas en TI (a través de boletines para clientes, asesoría o apoyo a sus mensajes publicitarios, por ejemplo), como para los propios medios de comunicación, bien sean de la fuente especializada o no.

    b. **Capacitación**. Empresas especializadas en capacitación, podrían obtener beneficios inmediatos al incorporar aspectos de seguridad en sus programas de enseñanza, dirigido a diferentes segmentos, tanto organizacionales como personales. Otras organizaciones, como son consultores, integradores, e incluso fabricantes y prestadores de servicios relacionados con la tecnología, podrían encontrar en esta actividad una forma de agregar valor a su oferta y de obtener ingresos adicionales.

2. La colaboración entre los diferentes proveedores de la industria, para crear soluciones completas sobre seguridad en informática para el cliente (integrando software y hardware en ambientes estandarizados o multiplataforma).

3. La creación de un mayor número de productos y servicios informáticos, que ya tengan incluidos elementos de seguridad.

4. Incluir, como parte de los productos o servicios ofrecidos por los proveedores de la industria, herramientas complementarias a los mismos, como pueden ser, por ejemplo, manuales de políticas y mejores prácticas para su utilización en un entorno de seguridad en informática.

Éstas son sólo algunas de las áreas de oportunidad de negocio que podrían desprenderse de los resultados de este estudio. Cada lector, cada empresario, podrá tener, a través de la visión particular de su mercado y de su negocio, una gama de múltiples opciones para incrementar su participación en este esfuerzo por colocar a México en un alto nivel en materia de Seguridad en Informática.

V. Artículos sobre Seguridad en Informática

1. Protección de datos "Off-Site", medida indispensable en todo DRP

Por Erwann Rehault
Desarrollo de negocio – División OSDP / Iron Mountain México / erehault@ironmountain.com.mx

¿Por qué las empresas del Primer Mundo respaldan y protegen su información "Off-Site"?

Independientemente del tamaño de cualquier empresa, o de su giro, la información electrónica representa una parte fundamental de todo negocio – en su operación diaria y para su propia supervivencia. Bases de datos, aplicaciones críticas, servidores, correo electrónico (e-mail), entre otros, son ejemplos representativos de la importancia que ha ido tomando la información electrónica en el ámbito comercial.

La pérdida de esta información, total o parcial, es un riesgo latente contra el cual las organizaciones deben lidiar día tras día. Por ejemplo, una falla de software o la caída de un servidor, puede paralizar completamente la operación de su negocio durante cierto tiempo – hasta restaurar nuevamente la información.

Como garantía de recuperación rápida, los expertos en la elaboración de Planes de Recuperación en caso de Desastres (DRP, por sus siglas en inglés) recomiendan a las empresas que procuren un servicio de Protección de datos "Off-Site" – del inglés *Off-Site Data Protection (OSDP)*. El servicio de OSDP es un elemento clave, que forma parte de cualquier DRP en la mayoría de las empresas de EUA o Europa. Sin embargo, en México, es un concepto desconocido y casi siempre omitido en los DRPs. Dos razones pueden explicar este fenómeno: por una parte, la escasa concientización y falta de cultura en cuanto a Seguridad en Informática en México, y, por otra, la insuficiencia de proveedores dedicados a Protección de Datos "Off-Site" en nuestro país.

Cuando hablamos de Seguridad de la Información en el ámbito de IT, se pueden clasificar las amenazas y riesgos más comunes en 3 categorías: fenómenos naturales, agresores internos y agresores externos.

Los fenómenos naturales constituyen amenazas obvias para la información. Incendios, inundaciones, humedad y plagas, entre otras, pueden dañar parcial o completamente su infraestructura de hardware y software operativo. Ante estos riesgos, el respaldo y la custodia de la información "On-Site" (en sitio), no es una medida preventiva suficiente, ya que los mismos respaldos pueden verse destruidos o dañados al igual que las instalaciones. Por lo mismo, y con el fin de evitar estos problemas, los expertos en DRP recomiendan que la información esté respaldada en un sitio externo – o sea "Off-Site" – a una distancia de mínimo 5 millas (8.04 Km aprox.) del Data Center de la empresa.

Los agresores internos forman el segundo tipo de amenaza más común. Empleados o ex-empleados de la empresa, suelen ser causa de daños, ya que, al tener acceso a la información crítica de la organización, pueden corromperla. Considérese también que la mayoría de los casos de robo o pérdida de información, tienen orígenes en el ámbito interno de la empresa. La implementación de una política de seguridad multinivel, con accesos restringidos para cierto tipo de información, permite reducir los riesgos de sabotaje o de errores humanos. Sin embargo, como garantía, muchas empresas optan por un nivel de seguridad adicional, respaldando y protegiendo su información fuera de sus instalaciones(Protección de Datos "Out of Reach"). De esta manera, la información confidencial de la empresa queda fuera de al-

cance, y no puede ser dañada – voluntaria o involuntariamente - por agresores internos.

Los agresores externos representan el tercer tipo de amenaza contra el cual las empresas modernas deben lidiar. Hackers y códigos dañinos (virus, gusanos, etc.), son los ejemplos más comunes para ilustrar este tipo de agresión. Algunas opciones de protección frente a estos agresores, son los conocidos "firewalls" y programas antivirus. Sin embargo, aun las redes más seguras están expuestas a la corrupción de la información. Por lo tanto, para salvaguardarla, la única y verdadera alternativa es el respaldo regular de la información y su conservación "Off-Line". Una vez más, los expertos en DRP recomiendan la Protección de Datos "Off-Site" como medida adicional para proteger la información y evitar cualquier tipo de desastre causado por un agresor externo.

En resumen, el respaldo y la protección de sus medios magnéticos (Información) "Off-Site", debería estar contemplado como parte indispensable de todo DRP, como una solución segura frente a las varias amenazas que pueden llegar a perjudicar cualquier negocio. Con el servicio de Protección de Datos "Off-Site", las empresas garantizan una recuperación rápida, independientemente del problema enfrentado, al contar con respaldos siempre actualizados de la información:

- Off-Site (fuera de sitio) = contra desastres naturales
- Off-Line (fuera de línea) = contra agresores externos, como hackers, o virus
- Out of Reach = contra agresores internos (sabotaje, etc)

2. Seguridad Informática, Disponibilidad de la Información y Continuidad de Negocios

Por José Fonseca
Director de Outsourcing / Kio Networks / jfonseca@kionetworks.com

La información es una de las partes fundamentales del capital de las organizaciones. Por lo mismo, debe resguardarse de la misma manera que cualquier otro tipo de capital y fluir hacia los interactuantes operativos y estratégicos, previamente definidos, en los momentos en que ésta sea requerida. Esto quiere decir que la Seguridad de la Información, en términos de negocios, no se limita al resguardo y aislamiento de los datos y su infraestructura; su ámbito tiene que ver también con la **Disponibilidad** de la información y la **Continuidad** del negocio mismo.

La adopción de componentes aislados, como programas antivirus o firewalls, permite eliminar sólo una fracción de la vulnerabilidad. Hoy sabemos que menos del 15% de las amenazas de este tipo, pueden ser eliminadas con estas herramientas.

Los mecanismos que se adopten, deben reunir una serie de componentes para asegurar la aplicación de un blindaje integral que garantice seguridad, disponibilidad y continuidad en el uso de recursos informáticos. Los más importantes, son:

1. Política de Seguridad de la Información.
2. Capacitación y difusión permanente de políticas y procedimientos.
3. Asignación de responsabilidades de seguridad.
4. Sistema de detección física y reporte de incidentes de seguridad.
5. Sistema de detección y control antivirus.
6. Proceso de planeación de continuidad del negocio e infraestructura de recuperación.
7. Herramientas de monitoreo y control de activos informáticos.
8. Alternativa de tercerización (outsourcing).

Uno de los principales recursos que permiten reducir la vulnerabilidad por acciones negligentes, accidentales o deliberadas, es el diseño de **políticas y procedimientos de seguridad de la información**, las cuales deben ser comunicadas y establecidas como obligatorias en todos los niveles de la organización. Éstas deben ser consistentes con los riesgos, los límites de vulnerabilidad, las necesidades de disponibilidad y los requerimientos de recuperación para la continuidad de las operaciones.

Más del 85% de las fallas de seguridad en informática se deben a errores, omisiones o actos deliberados del personal interno o de usuarios autorizados. Las herramientas de **capacitación y divulgación**, en este sentido, son fundamentales para mejorar la seguridad de las organizaciones. Ahora bien, una capacitación programada y una estrategia adecuada de difusión, no son suficientes por sí solas. Cada uno de los miembros de la organización juega un papel relacionado con la seguridad, por lo que resulta indispensable que haya una asignación precisa de **funciones** y división de **responsabilidades**, para observar y verificar las prácticas que se realizan en este sentido.

Los sistemas de **detección, monitoreo** y **automatización**, deben formar parte de la infraestructura de protección de la información. Por un lado, se encuentran los mecanismos de **identificación y restricción de acceso** a las instalaciones, como puertas, exclusas, dispositivos sensibles al movimiento, circuitos cerrados de televisión, tarjetas de proximidad, mecanismos de identificación biométrica y fotográfica, con las herramientas de software y hardeware necesarias, entre otros. Asimismo, se debe contar con sistemas de detección y control de accesos electrónicos, como los conocidos **Firewalls** y **Antivirus**.

Hasta aquí, se puede constituir una infraestructura básica de Seguridad de la Información, prácticamente accesible, en términos de costos, a cualquier empresa o institución. Son medidas preventivas que, si bien demandan planeación y organización por parte de los responsables del negocio y de todos los recursos humanos, pueden ser implementadas con cierta facilidad.

Ahora bien, en términos del negocio, ¿Qué sucede si surgen eventualidades, como una falla de energía, un incendio o simplemente una descompostura? ¿Qué tan importante es que la información sea accesible todo el tiempo? ¿Cuál es el costo de que "se caiga el sistema" y cuánto tiempo está dispuesta la organización, o sus clientes, a permanecer sin acceso? Es aquí donde se trasciende el concepto de "Protección", para dejar paso al de "**Disponibilidad**" y "**Continuidad de la Operación**".

La relación Costo-Riesgo es algo que debe realizarse cuidadosamente, ya que la infraestructura necesaria para sostener la operación del negocio en forma permanente, puede requerir desde miles hasta millones de dólares. Habrá negocios para los que una planta de luz de cierta capacidad, pueda ser suficiente. Sin embargo, otras organizaciones con grandes volúmenes de transacciones o una alta responsabilidad frente a sus usuarios, podrían necesitar apoyos tecnológicos de alta precisión y gran envergadura, para mantener sus componentes críticos en actividad durante las 24 horas del día, los 7 días de la semana y los 365 días del año. Hay que contemplar que, cuando la infraestructura tecnológica en su conjunto o alguno de sus componentes críticos falla, es preciso contar con mecanismos alternos de recuperación, cuyo costo asociado dependerá de la criticidad y el nivel de dependencia de la tecnología para continuar con la operación del negocio. Entre estas soluciones, se encuentran dispositivos de monitoreo y control de los activos informáticos, infraestructura fina y completa en los centros de cómputo y telecomunicaciones, recursos humanos especializados, metodologías, procesos y herramientas, etc. Todos estos elementos se definen en un **Plan de Continuidad del Negocio** (BCS, por sus siglas en inglés), en conjunto con un **Plan de Recuperación en caso de Desastre** (DRP).

La ventaja del Outsourcing

Ante los altos costos que para una sola empresa puede implicar el fortalecer las bases de la infraestructura para obtener un servicio realmente 24x7x365, existen empresas que hacen grandes inversiones en instalaciones de misión crítica y en la integración de equipos de profesionales altamente calificados, a fin de poder entregar servicios que conlleven todos los elementos esenciales de la seguridad informática, en su ámbito más amplio de alcance. Algunos proveedores de servicios tercerizados de tecnología de información y telecomunicaciones, pueden garantizar una disponibilidad de hasta 99.999%, lo que significa tener permanentemente disponible la infraestructura de cómputo, con un margen permitido de 5 minutos del total de minutos de todo un año. Tal es el caso de Kio NetWorks, único complejo de instalaciones de centros de datos en México, capaz de ofrecer ese nivel de disponibilidad.

Bajo este esquema, empresas de diversos tamaños y con distintas necesidades, pueden acceder a estándares muy altos en materia de seguridad y utilizar herramientas complejas y costosas para administrar su información estratégica, por una fracción de lo que le costaría a la organización sostenerlas.

3. Vilsa: prevención de riesgos y vanguardia tecnológica

Por Luis Raúl Vidales
Director General / Grupo Vilsa / lvidales@vilsa.com.mx

Vilsa ha desarrollado una amplia experiencia en sistemas de prevención de riesgos, con base en tecnologías de vanguardia. Esta empresa mexicana ha desempeñado un rol fundamental alrededor de la seguridad, en eventos internacionales de la magnitud de la Quinta Reunión Ministerial de la Organización Mundial de Comercio, celebrada en la ciudad de Cancún (2003), o la III Cumbre América Latina y El Caribe — Unión Europea que se realizó el pasado 28 de mayo en Guadalajara.

Bien puede hablarse de un récord, a lo largo de los años en que el Grupo Vilsa ha desarrollado su labor de prevención de riesgos, donde ha participado en el resguardo de la seguridad de 148 jefes de estado y 151 ministros y altos funcionarios del gobierno de México y otros países.

Esta labor ha sido posible realizarla con la suma de las más diversas tecnologías de vanguardia, que el Grupo Vilsa logró integrar en sistemas de prevención de riesgos y sofisticados servicios de seguridad del más alto nivel.

La primera experiencia del Grupo Vilsa en eventos de importancia internacional, fue en 1990 cuando se celebraron en México los XVI Juegos Centroamericanos y del Caribe. A lo largo de los años, esta empresa mexicana, líder en el rubro de la prevención de riesgos, ha diseñado eficaces sistemas de seguridad en reuniones cumbre, como la X Reunión de los líderes de la Asia-Pacific Economic Cooperation, realizada en el año 2002 en Los Cabos.

El Grupo Vilsa es precursor en la instrumentación y operación de los Sistemas de Reconocimiento Facial, lo que le ha permitido desarrollar operaciones de control de acceso con éxito en estos importantes eventos.

En cada ocasión el reto ha sido lograr que la seguridad no dificulte el desarrollo de estas importantes reuniones a nivel internacional, y que resulte un valor agregado de eficiencia para lograr los mejores resultados.

En Guadalajara, cuando fue la celebración de la III Cumbre América Latina y El Caribe — Unión Europea, se implementó un sistema de control de acceso basado en acreditaciones con fotografía, elaboradas en tarjetas de alta seguridad. Se trata de la más moderna tecnología (Contacless y Laser), instalada en un sistema dinámico y amable, que resultó eficaz para el control del aforo al Instituto Cultural Cabañas.

El Sistema de Reconocimiento Facial es una operación que dura fracciones de segundo y que permite comparar, contra el banco de datos, la fotografía que presenta la acreditación, con lo que se logra un amplio registro de los participantes y se detecta a las personas que sin la acreditación pertinente intentan tener acceso a áreas restringidas. Se trata de un acceso tan seguro como ágil, parte esencial de un sistema de seguridad inteligente y amable.

Recientemente el Grupo Vilsa fue reconocido a nivel internacional por Datacard Group, quien concedió a esta empresa mexicana dos reconocimientos por Exceptional Achivement (Logro excpecional). Hatim Tyabji, uno de los más altos funcionarios de Data Card Group, otorgó a Vilsa los preciados reconocimientos President´s Achiever Award y President´s Alliance Award.

Lo que sustenta los servicios que ofrece el Grupo Vilsa en distintos rubros de la prevención de riesgos, es la calidad de sus proveedores. Empresas líderes a nivel internacional, que le permiten integrar sus productos en tecnología de vanguardia, como los sistemas de Reconocimiento Facial. En esta integración es determinante la preparación y creatividad de los expertos de Técnica Comercial Vilsa.

Técnica Comercial Vilsa, simiente del Grupo Vilsa, fue fundada en 1982 con el propósito de generar servicios de seguridad basados en tecnología de vanguardia.

Vilsa posee una vasta experiencia en instalación de sistemas de seguridad, tanto en el sector público como privado, y ha desarrollado innumerables sistemas de identificación, acceso y resguardo de información. A lo largo de los años, esta empresa ha ofrecido servicios integrales de seguridad. Una empresa mexicana con reconocimiento a nivel mundial.

4. Guía Rápida de Políticas de Seguridad

Por John Serrano
Director General / Joint Future Systems, S.C. / jserrano@jfs.com.mx

Elementos que conforman la seguridad en informática

La seguridad en la informática debe apoyar la misión de la organización

El propósito de la seguridad en informática es salvaguardar la información y los bienes de una organización, por medio de la selección y la aplicación de medidas apropiadas. En su sentido más amplio, la seguridad en informática ayuda a la organización a proteger sus bienes físicos y financieros, su reputación y todos sus activos y recursos tangibles e intangibles. La seguridad es un medio, no un fin. Los procedimientos que se implementen no son universales ni generalizables, sino que tienen que ver con el desarrollo y la búsqueda de sincronía con la misión y propósitos de la organización.

La seguridad en informática es parte integral y fundamental de las directrices de la organización

Los sistemas de información y de computación son, cada vez más, elementos críticos en la estrategia y funcionamiento de las organizaciones. Su protección es prioritaria para garantizar el buen funcionamiento y el cumplimiento de metas de la organización.

La seguridad en informática tiene que ser costo-efectiva

La relación costo-beneficio de un sistema de seguridad, debe ser examinada con toda atención, tanto en sus consecuencias monetarias como en términos no monetarios, para asegurar que el costo no exceda los beneficios esperados. Invertir en medidas de seguridad en informática reduce la frecuencia y la severidad de los daños en cualquier ámbito; cuánto invertir y en qué, dependerá precisamente del valor (en tiempo y dinero) de lo que se quiera proteger, en relación con el costo de hacerlo. No puede ser más caro un sistema de seguridad, que el valor de la información que busca proteger, por lo que se requiere la realización de estudios serios de niveles de riesgo antes de implementar una política general de seguridad en informática.

La seguridad en informática debe ser multinivel

El concepto "multinivel" en materia de acceso, es igual al que se hace rutinariamente en un espacio físico. Por ejemplo, en un banco toda persona tiene acceso a las ventanillas desde afuera, algunas personas tienen acceso a las ventanillas por dentro y un número muy reducido de personas tienen acceso a la bóveda. Este criterio se utiliza en las empresas para aislar áreas de información, la cual se clasifica por niveles de confidencialidad. Una vez clasificada la información, se implementan los procedimientos físicos, de equipamiento y de configuración que se requieren para cada nivel. Una correcta clasificación de información y su ubicación en el nivel de seguridad que le corresponde, resulta en un esquema de seguridad eficiente y práctico. Las medidas de seguridad en informática que pretenden cubrir demasiado, entorpecen y encarecen la operación de un organismo y se convierten, paradójicamente, en un riesgo de seguridad, al ampliar la cantidad de personas que requieren conocer claves y procedimientos de acceso.

Por otra parte, la totalidad de los accesos informáticos a los sistemas de una organización debe estar distribuida entre diversas personas. Esto reduce la posibilidad de robo y fraude, al tener que estar involucradas múltiples personas para llevarlos a cabo, y evita que una sola persona pueda ser percibida como blanco de ataque por parte de agresores.

La seguridad en informática debe ser evaluada y modificada periódicamente

Los equipos de cómputo, telecomunicaciones y el ambiente en el que trabajan, son dinámicos. La tecnología, los usuarios, la información, los peligros y riesgos, cambian constantemente, lo que puede ocasionar que los programas de seguridad implementados pierdan vigencia y, por consiguiente, efectividad. Existe la necesidad de elaborar un calendario de evaluación periódica en relación con los sistemas de seguridad.

Los programas de seguridad en informática, no pueden ser estáticos y deben modificarse de manera permanente, ya que a medida que los procedimientos comienzan a ser rutinarios, inicia un natural relajamiento por parte de quienes los vigilan y, al mismo tiempo, posibles agresores podrían haber ya evaluado su funcionamiento y encontrado puntos de vulnerabilidad. Precisamente la búsqueda de los huecos de seguridad debe ser una función continua dentro de una organización. Si ésta no los encuentra, sus agresores seguramente lo harán.

La seguridad en informática y los derechos humanos

Uno de los obstáculos mayores para lograr establecer sistemas de seguridad efectivos, es la cuestión social. ¿Dónde interfiere el sistema de seguridad con los derechos de los trabajadores? ¿Pueden los sistemas de seguridad interferir con el derecho a la privacidad? ¿Qué se debe hacer? El principio básico es que las medidas de seguridad deben ser implementadas tomando en cuenta los derechos e intereses de todos los involucrados. Esto tiene que ver con balancear las necesidades de seguridad con los supuestos sociales. Por otro lado, se debe entender que por definición las relaciones entre seguridad y derechos humanos no son necesariamente antagónicas. De hecho, un sistema de seguridad bien implementado puede incluso aumentar el nivel de privacidad y de respeto de los empleados.

Distribución de responsabilidades en Seguridad en Informática

La asignación de funciones y responsabilidades en seguridad en informática, debe ser clara y explícita. Si bien el tamaño de la organización y la importancia de la información determinarán las características específicas del programa de seguridad en informática, en todos los casos deberá quedar establecido y documentado claramente quiénes son los responsables de cada parte y cuáles son sus funciones específicas.

En general, los puestos que tienen que ver con los procesos de seguridad son:

Director general

La responsabilidad última recae siempre en la dirección general. No se puede implementar ningún sistema de seguridad sin su aprobación y apoyo. La dirección general establece los niveles de seguridad, los propósitos, objetivos y prioridades, lo cual no quiere decir que deba tener claves de acceso informático a todos los sistemas, por la seguridad de la organización y del mismo director general. Es quien, en primer lugar, tiene la responsabilidad de dar un buen ejemplo a los empleados, siguiendo las pautas y reglas establecidas.

Director de sistemas

Si bien la dirección general es en quien recae la responsabilidad final, es en la dirección de sistemas donde el proceso y metodología se imple-

mentan. La dirección de sistemas tiene un reto doble: mantener la eficacia en el manejo y flujo de información para las otras áreas y utilizar un sistema de seguridad confiable, que no entorpezca la operación.

Proveedores de tecnología

En el mundo globalizado en el que vivimos, donde enormes cantidades de información están al alcance de todos, es más importante que nunca mantener una relación de asociados con los proveedores de tecnología y conocer las medidas que ellos mismos aplican a sus sistemas de seguridad, confiabilidad de sus tecnologías, etcétera. El personal de cómputo de la empresa (programadores, técnicos, personal de *"help desk"*), debe ser considerado también como proveedor de tecnología, el cual tiene que estar enterado y capacitado respecto de los procedimientos y políticas de seguridad en informática en sus lugares de trabajo. Son ellos quienes operan y proveen de una mayor eficiencia a los procesos que se han decidido implementar.

Áreas de apoyo

Un sistema de seguridad en informática es un todo y las áreas que lo conforman deben tener una función y asignación de responsabilidades específica. Las áreas más comunes de apoyo son:

- **Seguridad de la empresa:** responsables del acceso y salida tanto de personas como de bienes.
- **Auditores:** Responsables de vigilar la eficiencia y estado de los sistemas de cómputo, así como de los equipos
- **Personal encargado de recuperación en caso de desastre:** Algunos organismos tienen personal dedicado a identificar y planear qué hacer en casos de desastres naturales. Esta área debe incluir planes de recuperación para los sistemas de información de los organismos, así como planes de continuidad de servicios de negocio.
- **Control de calidad:** El área de control de calidad tiene la responsabilidad de incluir los sistemas de seguridad en todos los procesos de calidad que se vayan a implementar.
- **Personal:** El área de personal deberá conocer el sistema de seguridad que se haya implementado en la organización e incluirlo en los manuales y dinámicas de inducción que se realicen para los empleados nuevos, así como en los programas de entrenamiento y capacitación que se tengan planeados para el personal de la organización.
- **Usuarios**. Es con ellos donde, al fin y al cabo, se comprueba si el sistema elegido funciona correctamente. ¿Conocen las reglas y procesos del sistema de información? ¿Los siguen efectivamente? ¿El sistema es sencillo de operar? ¿Han existido más problemas de seguridad desde que el sistema se implementó, se han reducido o han continuado igual?

Las amenazas y riesgos más comunes

Hay tres tipos de agresores:

Fenómenos naturales

Los fenómenos naturales, como incendios, temblores, inundaciones, humedad, plagas, etc., son riesgos que deben ser contemplados en todo sistema de seguridad. Por ejemplo, la localización geográfica donde se encuentre el centro de cómputo, deberá tomarse en cuenta en cualquier proceso de construcción, asignación o reubicación.¿Es un sitio húmedo? ¿Está localizado cerca de edificios de alto riesgo, como fábricas, refinerías, depósitos de combustible u otro tipo de almacenes? ¿Se encuentra en la ciudad o en el campo? ¿Se encuentra localizado en una región de temblores frecuentes? La cantidad de insectos o roedores en la región puede afectar la información tanto física, como los sistemas

electrónicos. Hallar las respuestas a este tipo de preguntas podrá fortalecer y mejorar el sistema de seguridad que se decida implementar.

Agresores internos

Robo y Fraude: Como ejemplos comunes, individuos pueden modificar el sistema de nómina y "reestructurar" sus contratos personales, asignándose a sí mismos dinero que el organismo no había presupuestado para ellos. Sistemas que miden el nivel de puntualidad, bonos, etcétera, corren el mismo peligro. Como es obvio, este tipo de crimen lo comete personal de la empresa, agresores internos, así como el robo físico de equipos de computación y periféricos, extracción de información estratégica o confidencial, etc.

Sabotaje: Los agresores internos representan un riesgo de sabotaje. Después de todo, empleados o ex-empleados de una organización, conocen el funcionamiento y las "debilidades" que la empresa u organismo tiene. Son ellos los que, en un momento dado, pueden sabotear un sistema. ¿Cuál es el perfil de este tipo de individuos? Por lo general, son personas que sienten que han sido agredidos, ignorados o violentados por los directores y jefes del organismo, aquéllos que sienten que la organización está en su contra, se perciben como traicionados o que la organización tiene una deuda con ellos.

Agresores externos

Hackers: El "*hacker*", (viene originalmente de un término en inglés que se refiere a una persona que utiliza un hacha para destrozar o construir algo) es aquél que logra entrar en un sistema de computación sin estar autorizado. Algunos *"hackers"* se especializan en un área específica, como obtención de claves de usuario, o algoritmos de encripción. Algunos expertos en computación consideran que el término "*hacker*" no implica un mal uso, y que un "*hacker*"que hace daño debe ser llamado un "*cracker*". Para propósitos de seguridad en informática, cualquier persona que llega o dispone de información a la que no tiene derecho, y que no pertenece o ha pertenecido a la organización, es considerado un agresor externo. Aunque un "*hacker*"puede ser un agresor interno, por lo general son externos. Frecuentemente el "*hacker*" ataca por afición, para demostrar que él puede penetrar cualquier sistema o para obtener una ganancia específica. Los programadores de virus, por ejemplo, son considerados agresores externos. Aunque los agresores externos representan cierto grado de riesgo, el peligro es generalmente menor al del agresor interno.

Ingeniería Social: Una arma que los agresores externos utilizan, además de sus herramientas tecnológicas, es la manipulación de personas. Un caso famoso a principio de los 90's, ocurrió cuando alguien habló a una compañía telefónica preguntando por el director del área de programación de teléfonos, fingiendo no recordar su nombre y tartamudeando un poco. "Necesito hablar con el Sr... este... ¿cómo se llama?.. el que lleva todo lo de programación de teléfonos..., El Sr..." La operadora, solícita, le preguntó "El Sr. X? "Si, él, señorita, gracias" contestó el "*hacker*". Posteriormente llamó al área de programación y pidió hablar con el responsable en turno. Cuando le contestó, el "*hacker*" le dijo: "Necesito urgentemente la lista de códigos de programación. Estoy hablando por instrucciones del Sr. X. Él me dijo que llamara y le solicitara a usted que me los envíe por e-mail inmediatamente." Una vez que recibió los códigos, el "*hacker*" participó en varios eventos que provocaron caídas fuertes del sistema telefónico en Estados Unidos, además de que compartió los códigos con todos sus amigos, a través de boletines electrónicos y sitios de mensajes (precursores de lo que ahora son los grupos de noticias en el World Wide Web). Los agresores externos se valen de muchos trucos para obtener la información directamente de las personas que trabajan en organizaciones y utilizan prácticas que van desde la extorsión hasta la seducción para obtenerla. El éxito de virus recientes como MyDoom y Netsky,

están basados en frases que inteligentemente provocan que los usuarios abran correos que no deberían, apelando a su curiosidad.

Espionaje industrial: El espionaje industrial es el acto de robar información confidencial de una empresa, organismo o institución, para beneficiar a otra empresa. El espionaje industrial está aumentando. Se incluye espionaje industrial en el rubro de agresores externos, sólo porque quien recibe los beneficios es precisamente el organismo o empresa rival, pero muchas veces se engaña, recluta o coerce a personal interno para que lleve a cabo las actividades de recopilación de información. Tres tipos de información sumamente susceptibles a ataques de espionaje industrial son: información financiera, listas de clientes e información sobre procesos de manufactura y desarrollo de productos.

Códigos dañinos: Los códigos dañinos son los famosos virus, gusanos, caballos de Troya, bombas lógicas y todo tipo de software que busca causar un daño en un sistema. Un virus es un segmento de código que responde copiándose a sí mismo en archivos ejecutables. Son programas diseñados para causar cierto daño específico y, sobre todo, para replicarse en la mayor cantidad de sistemas posible.

Lo que no es la seguridad

Los sistemas de seguridad que se implementen no deben ser obstáculos para la operación regular de la empresa u organismo. Si se diseña un sistema que entorpezca la operación y cause pugnas entre el personal, es un sistema fallido. Para garantizar la eficiencia y sobre todo el compromiso de las áreas de la empresa u organismo con el sistema, éste debe tomar en cuenta tres factores:

Productividad
Eficiencia
Derechos humanos

El primero que eliminará un sistema de seguridad que afecte la productividad de la institución, empresa u organismo, será el Director General. Por eso, es tan importante que la dirección establezca las premisas fundamentales de lo que buscan lograr con el sistema de seguridad y su incorporación, de forma sincrónica, con los procesos de la empresa.

Lo mismo se puede decir de la eficiencia. Los sistemas de seguridad no pueden afectar la eficiencia laboral. Por el contrario, un sistema de seguridad en verdad efectivo y valioso, logrará, de hecho, mayor eficiencia en los procesos y desarrollos del organismo. Por tal motivo, como se mencionó antes, el departamento de control de calidad deber ser un actor importante en el desarrollo y operación del sistema de seguridad.

Los derechos humanos se refieren a los derechos de los trabajadores y empleados. Los sistemas de seguridad, por costumbre, son mal vistos por los empleados. Surge consciente o inconscientemente la idea de que se implementa un sistema de seguridad porque "no confían en nosotros". Obligar a un empleado a, digamos, portar un gafete o mostrar el contenido de su bolso o portafolios, puede ser considerado como violencia por parte del empleador hacia él. La forma de evitar esto es capacitar al personal, que vean los dispositivos de seguridad como habilitadores, no como restricciones, y que conozcan por qué a todos les conviene que existan estos sistemas de seguridad. El incluir al personal en la solución y comunicarle efectivamente el motivo de establecer políticas y llevar a cabo las medidas de seguridad, ayuda a obtener su cooperación y elimina el riesgo de violaciones internas. Los directores deben ser los primeros en poner el ejemplo y ser ellos los que sigan las pautas y reglamentos.

Por otra parte, ningún sistema de seguridad puede ni debe ser violatorio de la intimidad del empleado. Hubo un caso muy famoso de una empresa en Estados Unidos que decidió, ante los robos que sufrían a diario de su material, poner cámaras de video en los baños. El asunto causó revuelo y los empleados demandaron a la compañía.

Un buen sistema de seguridad en informática, resulta en mayor productividad, eficiencia, ambiente de trabajo en equipo y puede ser la diferencia entre la supervivencia o extinción de una empresa u organismo.

El ABC del DRP

En materia de informática, un Plan de Recuperación en caso de Desastre (DRP por sus siglas en inglés), es el conjunto de documentos que especifican lo que debe hacer una organización para salvaguardar su información.

Generalmente se complementa con un Plan de Continuidad de Negocios (Business Continuity Plan), el cual se elabora para poder seguir operando los procesos críticos de la actividad propia del negocio, en caso de cualquier eventualidad. Imaginemos a una empresa con alto volumen de ventas y bajo margen. En caso de no poder atender a sus clientes como consecuencia de una caída de sus sistemas, podría tener pérdidas millonarias y tardarse mucho tiempo en volver al nivel de flujo de efectivo que tenía antes de la crisis. Cuando se dio el apagón en Estados Unidos en Agosto de 2003, se notó una falta de procedimientos de recuperación ante desastres en varios negocios. Muchos restaurantes, por ejemplo, al utilizar exclusivamente sistemas de cómputo para realizar el cobro a sus clientes, tuvieron que cerrar sus puertas, en vez de poner velas y cobrar manualmente, incluso con tarjetas de crédito, como se hace en muchos otros países. Además, se vieron obligados a tirar grandes cantidades de comida, por no contar con métodos alternos de refrigeración, almacenamiento o distribución.

Si bien, como lo denota su nombre, el documento habla de acciones a tomar una vez que ha sucedido algún problema, un DRP contempla muchas actividades de carácter preventivo. No basta con reaccionar para resolver los daños causados por alguna contingencia, sino que es necesario reducir las probabilidades de que ésta se produzca. Los costos implicados en ambas situaciones (resolver o evitar), pueden ser significativamente distintos. En informática aplica aún más que en muchas otras disciplinas, el adagio de "más vale prevenir que lamentar"

Los principales elementos que deben considerarse dentro de un DRP, incluyen:

Una descripción clara y concisa de los procedimientos de una organización.

Si no se sabe exactamente qué actividades tienen que realizarse, y en qué orden, es imposible reconstruir la operación de una organización. Mientras más claro tengan todos sus integrantes los procedimientos que deben restaurase (no únicamente electrónicos), más fácil será reanudar las actividades. Es importante que las personas responsables de la creación de un DRP distingan entre procesos y procedimientos. No se trata de hacer un tratado exhaustivo de todos los aspectos de una organización, para eso se tienen los diagramas de proceso utilizados generalmente en certificaciones tipo ISO. Lo que se requiere son procedimientos claramente definidos y descritos de la manera más concisa y específica posible.

Una clara relación de las responsabilidades y funciones de cada persona de la organización, en casos de emergencia.

Comenzando por la persona de mayor nivel jerárquico que pueda ser afectado por una emergencia, hasta la última persona en el organigrama, cada una debe estar capacitada y consciente de los resultados que se esperan de las acciones que tiene que llevar a cabo en determinados momentos de crisis. Esto incluye que cada persona sepa lo que tiene que hacer, a quién tiene que informar en cada etapa de la emergencia, así como las actividades que deben realizar sus subordinados y superiores inmediatos. En un caso ideal, cada persona dentro de la organización debe conocer el DRP completo. La única excep-

ción a esta regla es cuando algunos de los procedimientos tienen elementos de carácter confidencial, en cuyo caso esa parte del DRP sólo debe ser conocida por aquellas personas autorizadas para tener acceso a esa información (Need to know).

Definición de alternativas de recursos.

Se deben tener claramente identificadas las instalaciones físicas, proveedores, equipo de computo y comunicaciones, así como el personal al que una organización debe recurrir en caso de emergencias. En ocasiones implica utilizar recursos de la misma organización, reubicándolos, y en otras tener contratos establecidos con proveedores que puedan funcionar como auxiliares en estos casos.

Definición clara de fases de una emergencia.

Un DRP debe ser extremadamente claro respecto de lo que constituye cada fase dentro de una emergencia. En el momento en el cual se dan las condiciones para un cambio de fase, así la crisis se esté agravando o se esté resolviendo, se deben seguir los lineamientos puntuales que correspondan, tanto en lo que se refiere a las acciones a tomar como a la comunicación que tiene que darse en diversas direcciones.

Planeación de tiempos mínimos y máximos.

Cada paso de un DRP debe tener una estimación lo más exacta posible de los tiempos que va a tomar la realización de cada acción, estableciendo los máximos y mínimos. Esto se liga a la importancia de cada procedimiento, y debe tomar en cuenta las contingencias de cada evento aislado de recuperación.

Pruebas y modificaciones al DRP.

El plan debe probarse regularmente, con simulacros y evaluaciones documentales. Una organización no debe sólo crear un DRP, sino también establecer un programa de monitoreo y modificaciones. Al igual que otros aspectos de seguridad, un Plan de Recuperación en caso de Desastre es una actividad continua, con mejoras, cambios, ajustes y capacitación de personal.

El solo hecho de crear un DRP, es en muchas ocasiones un ejercicio muy útil para una organización. El poder reducir a su mínima expresión los procedimientos vitales y simplificar las relaciones que se dan entre los mismos, puede conllevar a una serie de mejoras a nivel de procesos, y aumentar la eficiencia y eficacia en todos los niveles de una organización.

Estudio
“Seguridad en Informática en México 2005”

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 será actualizado y publicado anualmente.

Con la experiencia obtenida en la realización de este estudio de percepción, y tomando en cuenta las sugerencias de algunos patrocinadores y amigos del ramo, a partir de octubre y durante los últimos meses de 2004, se estará efectuando el diseño, planteamiento metodológico y definición de patrocinios, para el desarrollo de la investigación de 2005.

Para mayor información, comuníquese a los siguientes teléfonos:

(55) 5286-1839
(55) 5286-6906

E-mail: market@jfs.com.mx

CAMEXA

CANIETI

EL UNIVERSAL

IRON MOUNTAIN

KIO NETWORKS

Política digital

Sun microsystems

symantec

Vilsa

JFS

JOINT FUTURE SYSTEMS, S.C.

Av. México 19-701
Col. Condesa
06100 México, D.F.
Tel. (55) 5286-1839
5286-6906
E-mail: market@jfs.com.mx
www.jfs.com.mx