Estudio de Percepción

Seguridad de la Información México 2011

JFS

JOINT FUTURE SYSTEMS

Datos
ersonales

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

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

CANIETI
www.canieti.org

KIO Networks

Secure Information Technologies

La Verdad nos hará libres
Universidad Iberoamericana
Ciudad de México

Empresas patrocinadoras

Cda. Popotla 11 – PB
Col. Popotla / Del. Miguel Hidalgo
11400 México, D.F.
Tel. (55) 5594-9257
correo@alapsi.org
presidencia@alapsi.org
www.alapsi.org

Centro Alemán – German Centre
Av. Santa Fe 170 piso 1-4-10
Col. Lomas de Santa Fe
01210 México, D.F.
Tel. 00 52 (55) 1500-5900
http://mexiko.ahk.de

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

Av. México 19 – 701
Col. Condesa
06100 México, D.F.
Tel. (55) 5286-6906 / 5286-1839
www.jfs.com.mx

Prolongación Paseo de la Reforma 5287
Cuajimalpa 05000 México, D.F.
Tel. 52 (55) 8503-2600
01 800 5 CALL KIO / 01800 522-5554
www.kionetworks.com

KIO Q
Cerrada de la Princesa 4
Municipio del Marqués, Qro.
Tel. 52 (55) 8503-2700
01 800 5 CALL KIO / 01800 522-5554
www.kionetworks.com

Josefa Ortiz de Domínguez No. 31
Col. Del Carmen Coyoacán 04100, México, D.F.
Tel. 52 (55) 5524-7582
Fax: 52 (55) 5524-8091
www.secureit.com.mx

Departamento de Ingenierías / Maestría en
Administración del Servicio de Tecnología de Información
Prol. Paseo de la Reforma 880
Lomas de Santa Fe 01219 México, D.F.
Tel. (55) 5950-4000 ext. 4720
www.uia.mx

Se agradece asimismo la ayuda de la Fundación Ealy Ortiz, A.C. y de la Academia Mexicana de la Comunicación, A.C.

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

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

ESTUDIO DE PERCEPCIÓN
SEGURIDAD EN INFORMÁTICA MÉXICO 2011

Ante la necesidad de contar con información específica de México, respecto de la percepción que sobre Seguridad en Informática tienen los usuarios de diferentes sectores, Joint Future Systems, en coordinación con otras organizaciones interesadas en la comprensión y difusión del tema, ha encabezado en diversas ocasiones la realización de un estudio enfocado a evaluar el grado de conocimiento y la percepción que existe al respecto, entre dos segmentos fundamentales: los usuarios corporativos e institucionales, así como expertos en la materia y proveedores líderes en el mercado de soluciones de Tecnología de la Información (TI).

Desde el año 2004 (cuando se llevó a cabo el primer Estudio de Percepción sobre Seguridad en Informática en México) a la fecha, la Seguridad de la Información, los conceptos alrededor de ella, la propia legislación sobre la materia y la percepción en general por parte de usuarios y expertos, ha sufrido cambios significativos. Lo que en aquel entonces se resumía prácticamente en virus, hackers, contraseñas y respaldo de discos, ha ido adquiriendo un espectro mucho más amplio de conceptos, al mismo tiempo que la jerarquía de las preocupaciones alrededor del tema se ha modificado. Todo esto, como consecuencia de los avances tecnológicos, de la forma en que trabajamos y nos comunicamos, así como de una mayor conciencia por parte de los usuarios de soluciones informáticas.

En los últimos meses de 2010 y principios de 2011, se llevaron a cabo las encuestas entre usuarios y especialistas para producir el **Estudio de Percepción sobre Seguridad en Informática México 2011**, con el propósito de dar continuidad a este esfuerzo por generar estadísticas del entorno de nuestro país en la materia, y de contar con parámetros comparativos que permitan vislumbrar las variaciones (avances o rezagos percibidos por los entrevistados).

Este estudio proporciona información recopilada de dos fuentes complementarias, lo que permite contemplar ambas perspectivas, tanto la del usuario común, como la del experto y proveedor de la industria.

Con la finalidad de que los lectores del presente documento obtengan información adicional, se seleccionó un tema asociado a la Seguridad de la Información que fuera relevante, en tiempo y forma, a lo que está aconteciendo actualmente en nuestro país. Es así que, dada la reciente publicación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, al final del estudio se incluye una sección con artículos sobre la **Protección de Datos Personales**, tanto en lo que toca a Particulares como a Dependencias, los cuales fueron escritos por personas de distintas organizaciones que, de una u otra forma, actúan o se ven afectados por las nuevas disposiciones.

Derivado de lo anterior, el contenido del estudio se ha clasificado de la siguiente manera:

A. Encuesta entre usuarios de diferentes áreas organizacionales, tanto de empresas privadas como de instituciones públicas.
B. Estudio de opinión y análisis con expertos en temas relacionados con seguridad en informática.
C. Artículos diversos acerca de la **Protección de Datos Personales**.

CONTENIDO

I. ALCANCES DE LA INVESTIGACIÓN TOTAL 6

II. INVESTIGACIÓN ENTRE EMPRESAS Y ÁREAS USUARIAS DE TI 7

OBJETIVOS DEL ESTUDIO 7

METODOLOGÍA 7

Método de investigación 7

Características de la muestra 7

Perfil de los entrevistados 7

Tamaño de la muestra 8

Codificación de respuestas 8

RESULTADOS 9

Composición de la muestra 9

Qué se entiende por "Seguridad en Informática" 11

Principales preocupaciones acerca de la Seguridad de equipos de cómputo y su contenido. 13

Amenazas de mayor riesgo para la Seguridad de la Información. 14

Normas y regulaciones de seguridad que conoce 16

Qué hace falta por parte de los proveedores de TI 18

Importancia de la Seguridad en Informática en las empresas 19

Aspectos a tomar en cuenta en la compra de tecnología 20

Percepción acerca de diversas marcas asociadas con Seguridad en Informática 22

Qué más les gustaría conocer acerca de Seguridad en Informática 25

III. ESTUDIO CON EXPERTOS Y PROVEEDORES LÍDERES DEL MERCADO TI 29

OBJETIVOS DEL ESTUDIO 29

METODOLOGÍA 29

Método de investigación 29

Relación de entrevistados 29

RESULTADOS 30

Situación de la Seguridad en Informática en México, frente a otros países del mundo 30

Principales retos de México como país, en materia de Seguridad en Informática 32

Principales retos de las organizaciones usuarias, en materia de Seguridad en Informática 33

Principales retos de los proveedores de hardware y software, en materia de Seguridad en Informática 34

Principales retos de las Instituciones Educativas mexicanas, en materia de Seguridad en Informática 35

Principales retos de los Medios de Comunicación, en materia de Seguridad en Informática 36

Principales retos del Gobierno de México, en materia de Seguridad en Informática 36

APORTACIONES RELACIONADAS CON SEGURIDAD EN INFORMÁTICA, REALIZADAS POR LAS EMPRESAS ENTREVISTADAS 38

ALAPSI 38

CommIT Service Management 38

Factory Tec *38*
Grupo Corporativo Diamante *39*
Instituto Federal de Acceso a la Información y Protección de Datos *39*
Integridata *39*
Institución financiera anónima *39*
Metronet *40*
Sentrigo *40*

IV. TEMA ESPECIAL DE LA EDICIÓN 2011: PROTECCIÓN DE DATOS PERSONALES 41

IMPLICACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES ENTRE LAS ORGANIZACIONES ENTREVISTADAS 41

OPINIÓN SOBRE LOS ALCANCES Y APLICABILIDAD DE LA LFPDPPP Y LA LFTAIPF 42

ARTÍCULOS ESPECIALES SOBRE LA PROTECCIÓN DE DATOS PERSONALES 45
Las Tecnologías de Información y la Lucha por la Privacidad *45*
Recomendaciones prácticas para la aplicación de la LFPDPPP *48*
México y el manejo de datos personales: El antes y el después de la Ley Federal de Protección de Datos Personales en Posesión de Particulares *59*
Autorregulación y sellos de confianza *61*
Pequeño Análisis a la Ley Federal de Protección de Datos Personales *64*
Cumplimiento con la LFPDPPP con el enfoque de Sistema de Gestión *66*
Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), un enfoque a la protección de bases de datos *70*
Protección de datos y el sistema de gestión *72*

I. ALCANCES DE LA INVESTIGACIÓN TOTAL

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

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

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

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

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

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

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

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

II. INVESTIGACIÓN ENTRE EMPRESAS Y ÁREAS USUARIAS DE TI

Objetivos del estudio

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

Metodología

Método de investigación

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

Posteriormente, se realizaron encuestas complementarias que permitieron cubrir una cuota mínima del 25% de entrevistados de la categoría **Informáticos** (26.8% real).

Características de la muestra

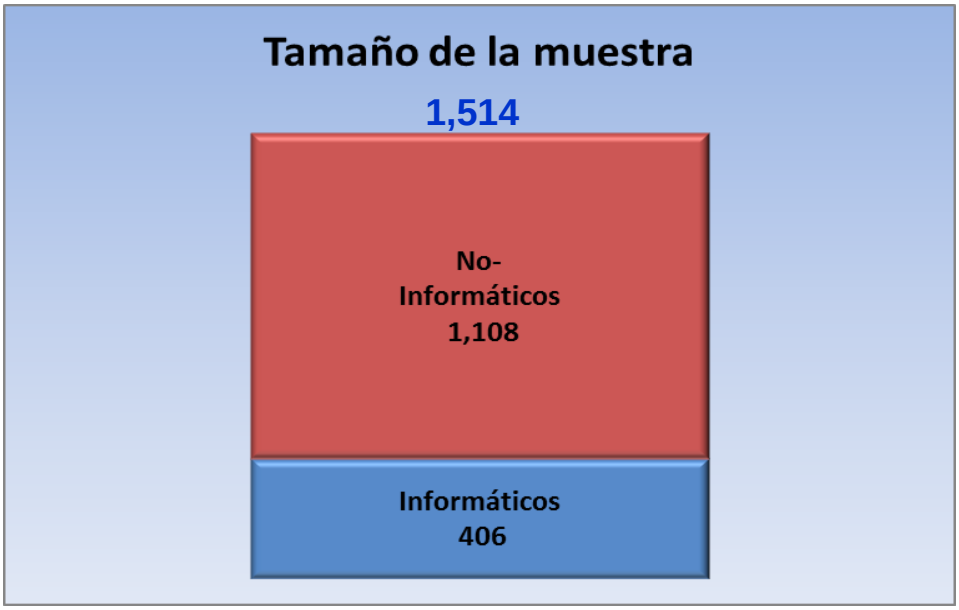
Se utilizó una muestra no probabilística, con las siguientes características.

Perfil de los entrevistados

Característica principal	Directivos y niveles medios de diferentes áreas organizacionales, de instituciones y empresas de todos tamaños.
Edad:	Indistinta

Sexo:	Indistinto
Cobertura geográfica:	Múltiple, dentro de la República Mexicana
N.S.E.	Indistinto
Especiales	1. Ser usuario de soluciones informáticas, con al menos 2 años de antigüedad. 2. Utilizar soluciones informáticas un tiempo mínimo de 10 horas semanales.

Tamaño de la muestra



GRÁFICA 1

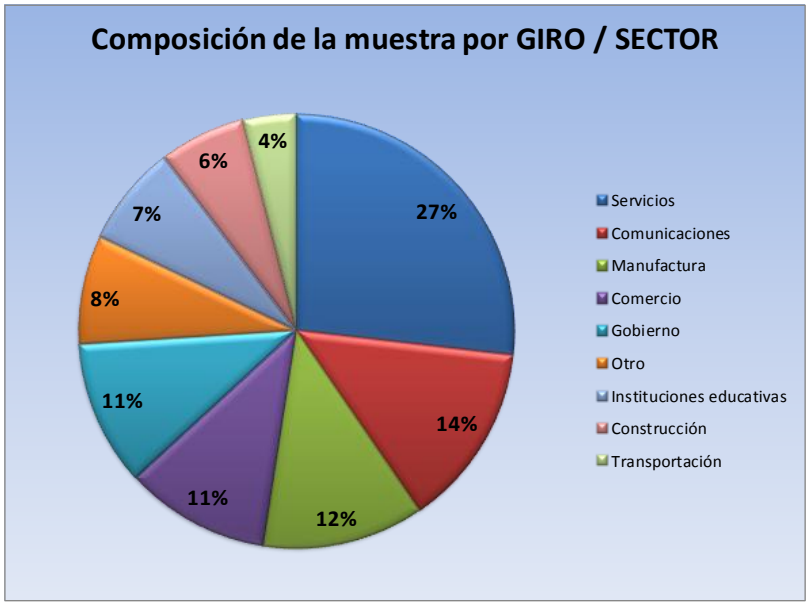
Codificación de respuestas

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

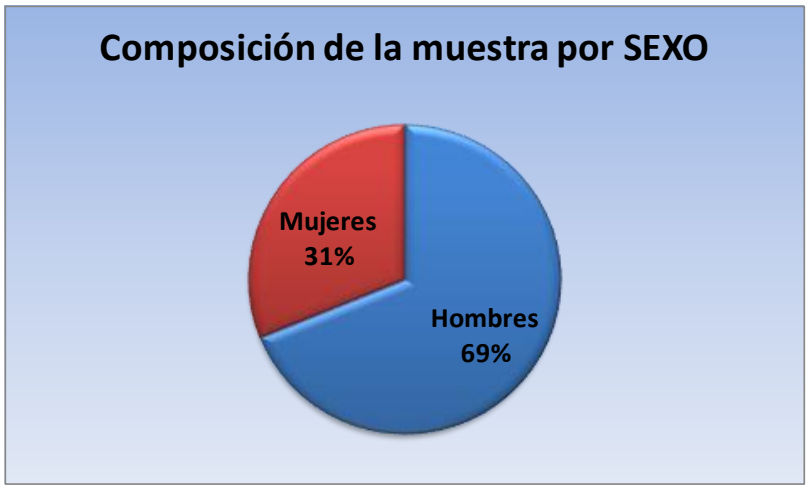
Resultados

Composición de la muestra

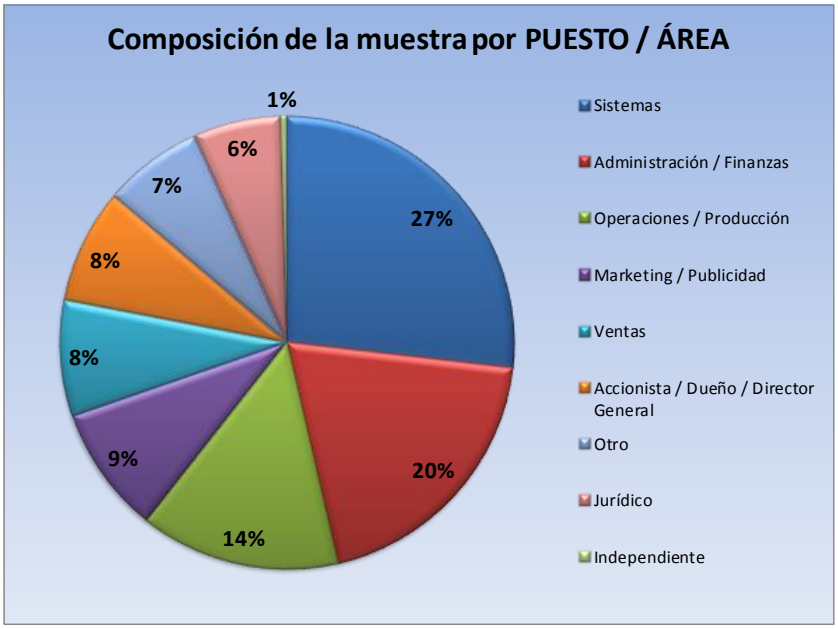
La composición de la muestra se clasifica bajo tres criterios – por sector, por sexo y por puesto o área de trabajo.



GRÁFICA 2



GRÁFICA 3


Composición de la muestra por PUESTO / ÁREA
1%
6%
7%
27%
8%
8%
9%
20%
14%
Sistemas
Administración / Finanzas
Operaciones / Producción
Marketing / Publicidad
Ventas
Accionista / Dueño / Director General
Otro
Jurídico
Independiente

GRÁFICA 4

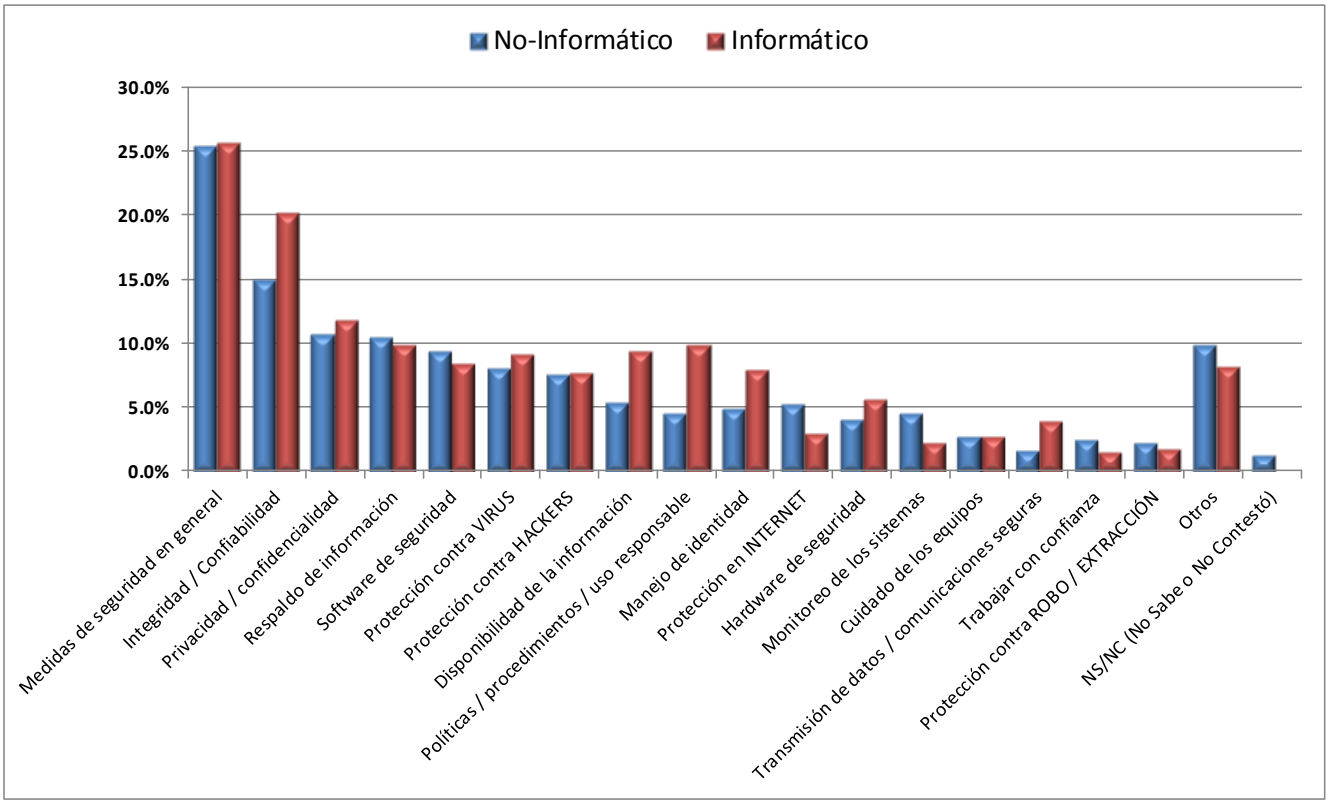
Qué se entiende por "Seguridad en Informática"

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 (1.39 respuestas promedio por entrevistado). La frecuencia de las respuestas ya codificadas, pueden apreciarse en la Tabla 1 y la Gráfica 5.

	No-Informático		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Medidas de seguridad en general	281	25.4%	104	25.6%	385	25.4%
Integridad / Confiabilidad de la información	166	15.0%	82	20.2%	248	16.4%
Privacidad / confidencialidad	119	10.7%	48	11.8%	167	11.0%
Respaldo de información	116	10.5%	40	9.9%	156	10.3%
Software de seguridad	104	9.4%	34	8.4%	138	9.1%
Protección contra VIRUS	89	8.0%	37	9.1%	126	8.3%
Protección contra HACKERS	84	7.6%	31	7.6%	115	7.6%
Disponibilidad de la información	60	5.4%	38	9.4%	98	6.5%
Políticas / procedimientos / uso responsable	51	4.6%	40	9.9%	91	6.0%
Manejo de identidad	55	5.0%	32	7.9%	87	5.7%
Protección en INTERNET	59	5.3%	12	3.0%	71	4.7%
Hardware de seguridad	45	4.1%	23	5.7%	68	4.5%
Monitoreo de los sistemas	50	4.5%	9	2.2%	59	3.9%
Cuidado de los equipos	30	2.7%	11	2.7%	41	2.7%
Transmisión de datos / comunicaciones seguras	18	1.6%	16	3.9%	34	2.2%
Trabajar con confianza	27	2.4%	6	1.5%	33	2.2%
Protección contra ROBO / EXTRACCIÓN	25	2.3%	7	1.7%	32	2.1%
Acceso físico controlado	15	1.4%	11	2.7%	26	1.7%
Garantía de continuidad en la operación	23	2.1%	2	0.5%	25	1.7%
Operaciones bancarias o de compra-venta seguras	20	1.8%	3	0.7%	23	1.5%
Protección de Datos Personales	13	1.2%	5	1.2%	18	1.2%
Protección contra FRAUDE o ENGAÑOS	10	0.9%	5	1.2%	15	1.0%
NS/NC (No Sabe o No Contestó)	14	1.3%	-	0.0%	14	0.9%
Spyware, protección contra	9	0.8%	4	1.0%	13	0.9%
Spam, protección contra	11	1.0%	1	0.2%	12	0.8%
Filtro de contenidos	6	0.5%	-	0.0%	6	0.4%
Protección en REDES SOCIALES	2	0.2%	1	0.2%	3	0.2%
Legislación sobre el tema	1	0.1%	-	0.0%	1	0.1%
Vigilancia	-	0.0%	1	0.2%	1	0.1%

TABLA 1 – QUÉ ES SEGURIDAD EN INFORMÁTICA



GRÁFICA 5 – QUÉ ES SEGURIDAD EN INFORMÁTICA

Coincidentemente con el estudio anterior, aunque no en el mismo orden, de manera general los tres principales conceptos asociados a Seguridad en Informática, son Medidas de seguridad en general, Integridad / Confiabilidad y Privacidad / Confidencialidad.

Destaca que el rubro de Políticas y Procedimientos, bajó en el ranking, pasando de la posición 5 en 2009 a la posición 9 en este estudio, siendo notoriamente un tema considerado en mucho mayor proporción por parte de los Informáticos que de los No-Informáticos.

Otra diferencia notable entre Informáticos y los No-Informáticos, es que los primeros toman más en cuenta aspectos como la Integridad y Confiabilidad de la Información, la Disponibilidad de la misma y el Manejo de Identidad, así como la Transmisión de Datos.

También resulta notorio que el rubro de Legislación sobre el tema de Seguridad de la Información, está en el último lugar con tan sólo una mención de entre más de 1,500 encuestados. Redes Sociales empieza a figurar entre las menciones de los entrevistados, aunque con una participación incipiente de apenas 3 menciones.

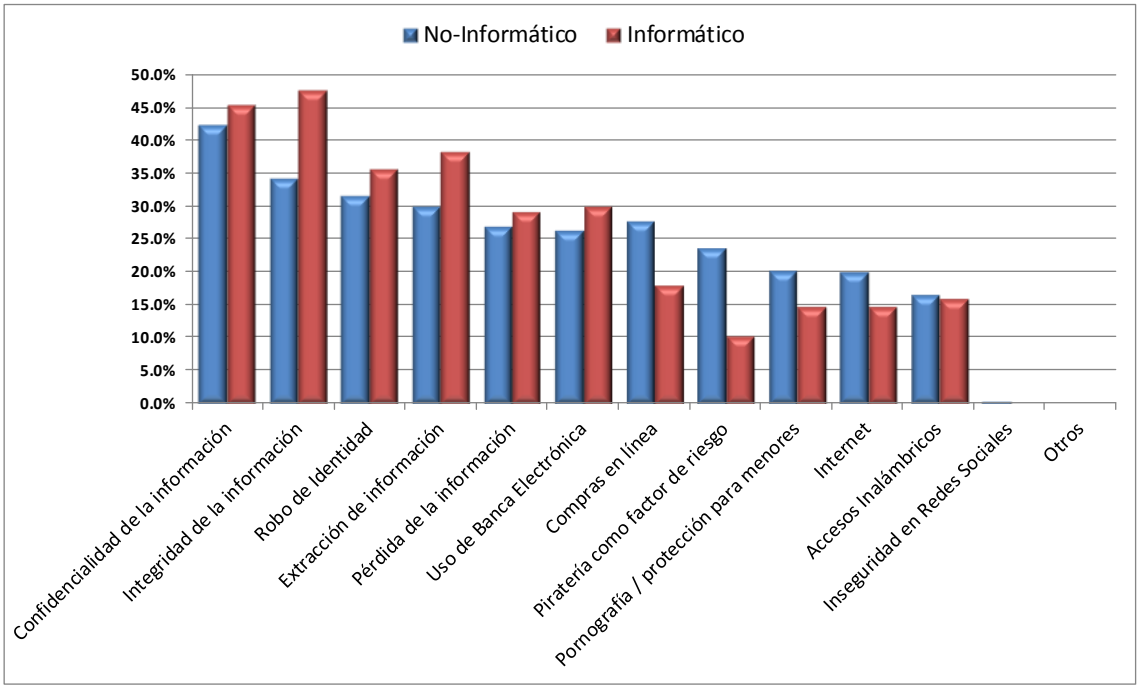
Principales preocupaciones acerca de la Seguridad de equipos de cómputo y su contenido.

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

En conjunto, las principales preocupaciones fueron como se describe en la Tabla 2 y en la Gráfica 6.

	No-Informáti		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Confidencialidad de la información	469	42.3%	184	45.3%	653	43.1%
Integridad de la información	379	34.2%	193	47.5%	572	37.8%
Robo de Identidad	350	31.6%	145	35.7%	495	32.7%
Extracción de información	332	30.0%	155	38.2%	487	32.2%
Pérdida de la información	298	26.9%	118	29.1%	416	27.5%
Uso de Banca Electrónica	291	26.3%	122	30.0%	413	27.3%
Compras en línea	307	27.7%	73	18.0%	380	25.1%
Piratería como factor de riesgo	262	23.6%	42	10.3%	304	20.1%
Pornografía / protección para menores	224	20.2%	60	14.8%	284	18.8%
Internet	223	20.1%	60	14.8%	283	18.7%
Accesos Inalámbricos	184	16.6%	65	16.0%	249	16.4%
Inseguridad en Redes Sociales	4	0.4%	1	0.2%	5	0.3%
Otros	1	0.1%	-	0.0%	1	0.1%

TABLA 2 – PRINCIPALES PREOCUPACIONES



GRÁFICA 6 – PRINCIPALES PREOCUPACIONES

Los tres rubros más significativos para ambos grupos, coinciden tanto en la temática como en el orden de prioridad, con los del estudio anterior. En primer lugar están Confidencialidad y Privacidad de la Información, seguida por la Integridad de la misma y en tercer lugar el Robo de Identidad.

Se percibe de manera particular que los temas que salieron con una mayor frecuencia de menciones, preocupan, en proporción, más a los Informáticos que a los no informáticos, mientras que los temas que en conjunto tienden a preocupar a menos personas, suelen preocupar más a los No-Informáticos. Entre ellos, las Compras en línea, la Piratería como factor de riesgo, la Pornografía y la Protección para menores y el uso de Internet.

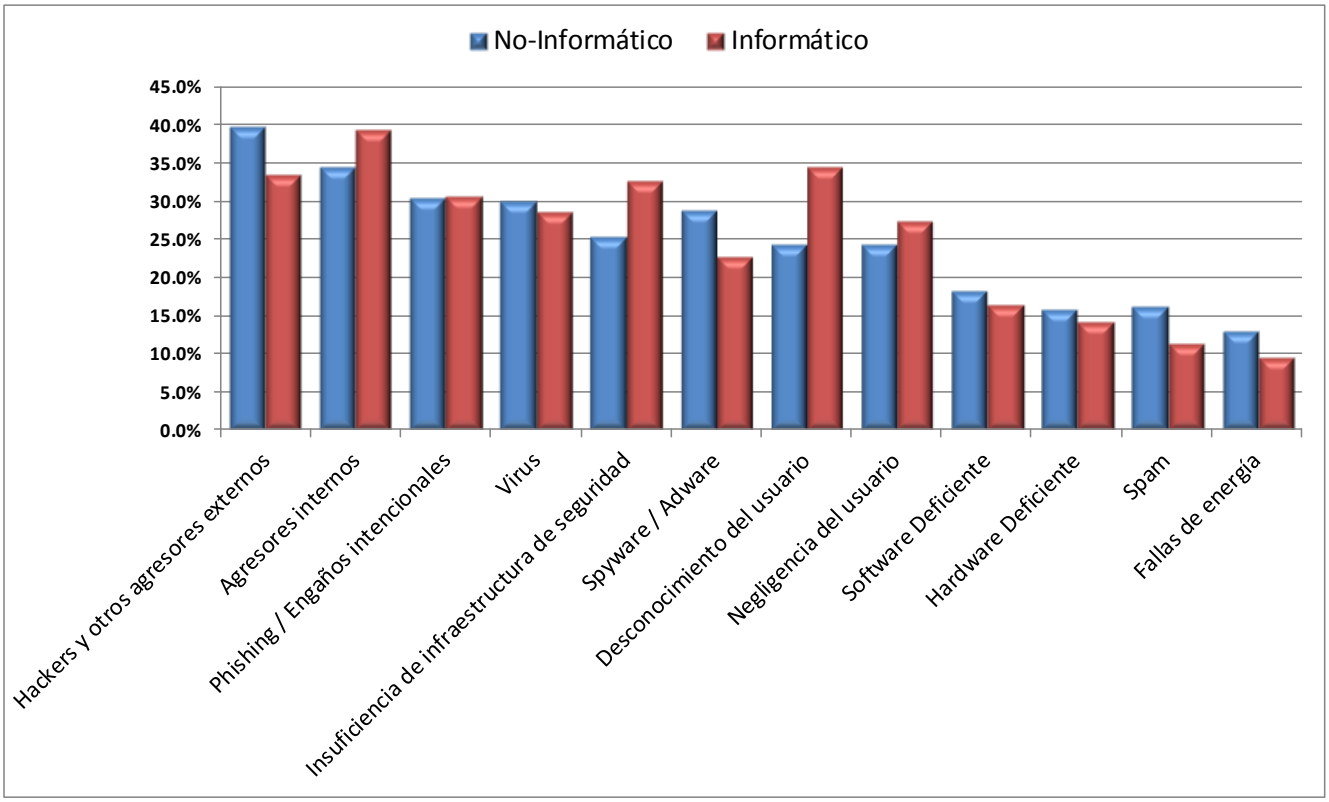
Amenazas de mayor riesgo para la Seguridad de la Información.

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

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

	No-Informáti		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Hackers y otros agresores externos	439	39.6%	136	33.5%	575	38.0%
Agresores internos	381	34.4%	160	39.4%	541	35.7%
Phishing / Engaños intencionales	337	30.4%	124	30.5%	461	30.4%
Virus	332	30.0%	116	28.6%	448	29.6%
Insuficiencia de infraestructura de seguridad	281	25.4%	132	32.5%	413	27.3%
Spyware / Adware	319	28.8%	92	22.7%	411	27.1%
Desconocimiento del usuario	269	24.3%	140	34.5%	409	27.0%
Negligencia del usuario	268	24.2%	111	27.3%	379	25.0%
Software Deficiente	201	18.1%	66	16.3%	267	17.6%
Hardware Deficiente	175	15.8%	57	14.0%	232	15.3%
Spam	178	16.1%	46	11.3%	224	14.8%
Fallas de energía	144	13.0%	38	9.4%	182	12.0%

TABLA 3 – AMENAZAS DE MAYOR RIESGO



GRÁFICA 7 – AMENAZAS DE MAYOR RIESGO

Es evidente que las principales amenazas consideradas por ambos grupos, tienen que ver de manera directa con acciones humanas malintencionadas, siendo los Agresores Externos o Hackers la amenaza considerada de mayor riesgo (mencionada por un 38% de los entrevistados), casi en la misma proporción que los agresores internos (35.7%). El Phishing y la Ingeniería Social aparecen en la tercera posición, acciones relacionadas ambas con los dos rubros mencionados en primer lugar. Una diferencia notable en esta evaluación, es que un número mayor de los entrevistados Informáticos considera a los Agresores Internos como una mayor amenaza, sobre los Agresores Externos, percepción que resulta inversa en el grupo de No-Informáticos.

Respecto del estudio anterior, sobresale que los Virus hoy en día son considerados como una amenaza menos peligrosa. En 2009 ocupaban la primera posición de menciones (principalmente para el grupo de los No-Informáticos) y este año quedan hasta la cuarta posición de menciones, superado por los 3 rubros ya comentados. Esto podría responder, o bien a que las nuevas tecnologías y el mejoramiento en el desarrollo de software permiten un mayor control de este tipo de amenaza, o a que las personas ven en los otros conceptos un riesgo aún mayor.

Asimismo se observa que para los Informáticos suelen ser amenazas de mayor peso, en proporción contra los No-Informáticos, conceptos como el Desconocimiento y la propia Negligencia de los operadores de soluciones informáticas, así como el contar con pocos recursos de infraestructura de seguridad.

Normas y regulaciones de seguridad que conoce

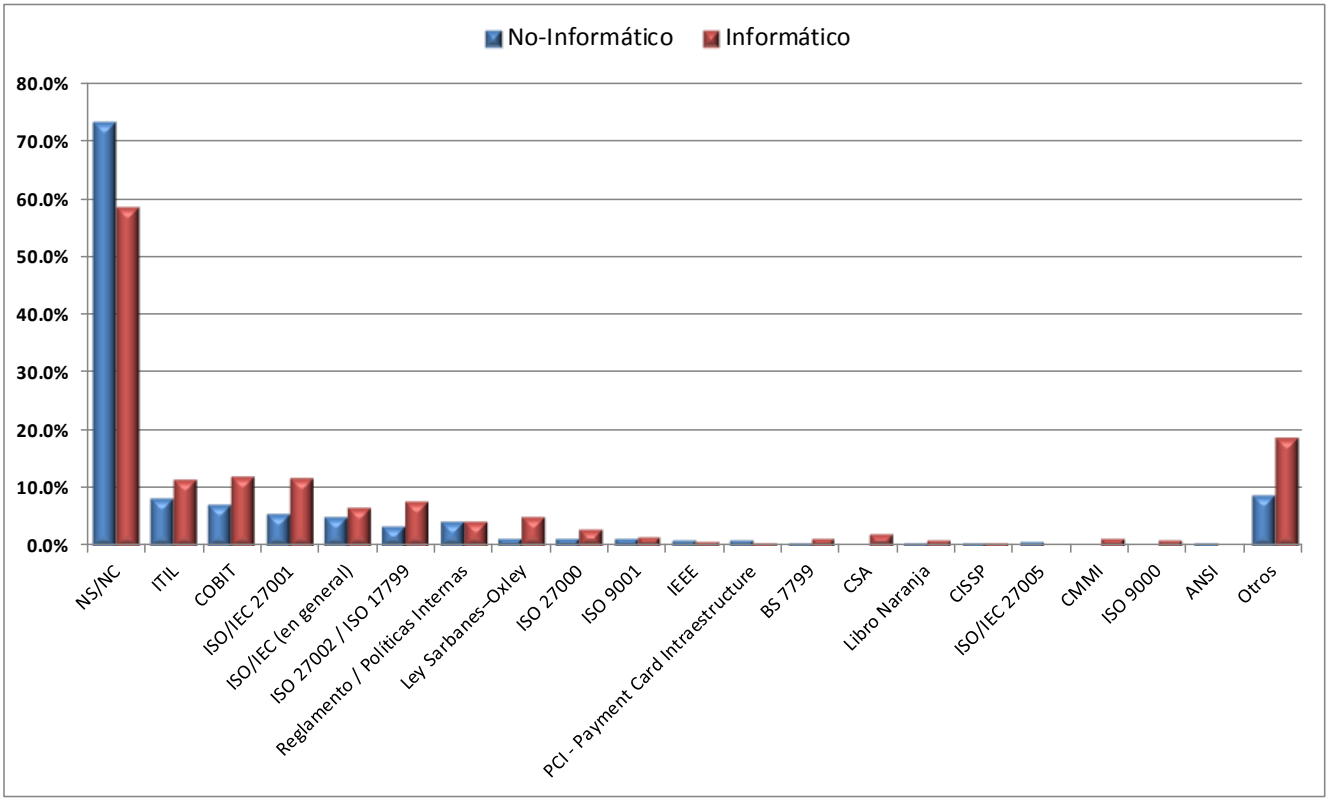
Pregunta: ¿Cuáles estándares, normas o regulaciones conoce, que mejoren la seguridad en informática?

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

TABLA 4

	No-Informático		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
NS/NC	812	73.3%	238	58.6%	1,050	69.4%
ITIL	92	8.3%	47	11.6%	139	9.2%
COBIT	80	7.2%	49	12.1%	129	8.5%
ISO/IEC 27001	62	5.6%	48	11.8%	110	7.3%
ISO/IEC (en general)	56	5.1%	27	6.7%	83	5.5%
ISO 27002 / ISO 17799	40	3.6%	32	7.9%	72	4.8%
Reglamento / Políticas Internas	48	4.3%	18	4.4%	66	4.4%
Ley Sarbanes–Oxley	17	1.5%	21	5.2%	38	2.5%
ISO 27000	15	1.4%	12	3.0%	27	1.8%
ISO 9001	16	1.4%	7	1.7%	23	1.5%
IEEE	12	1.1%	4	1.0%	16	1.1%
PCI - Payment Card Intraestructure	12	1.1%	3	0.7%	15	1.0%
BS 7799	8	0.7%	6	1.5%	14	0.9%
CSA	3	0.3%	9	2.2%	12	0.8%
Libro Naranja	7	0.6%	5	1.2%	12	0.8%
CISSP	8	0.7%	3	0.7%	11	0.7%
ISO/IEC 27005	10	0.9%	-	0.0%	10	0.7%
CMMI	3	0.3%	6	1.5%	9	0.6%
ISO 9000	4	0.4%	5	1.2%	9	0.6%
ANSI	8	0.7%	-	0.0%	8	0.5%
Derechos de autor	7	0.6%	1	0.2%	8	0.5%
BS 25999	6	0.5%	-	0.0%	6	0.4%
ISO 18000	3	0.3%	3	0.7%	6	0.4%
ISO 20000	2	0.2%	4	1.0%	6	0.4%
Las reglas del ISACA	3	0.3%	3	0.7%	6	0.4%
Ley de protección de datos personales (IFAI)	4	0.4%	2	0.5%	6	0.4%
NOM-151	3	0.3%	3	0.7%	6	0.4%
AZ/NZ4360	3	0.3%	2	0.5%	5	0.3%
HIPPAA	5	0.5%	-	0.0%	5	0.3%
ISO 7498	4	0.4%	-	0.0%	4	0.3%
NIST	-	0.0%	4	1.0%	4	0.3%
Norma A y B para cableado estructurado	1	0.1%	3	0.7%	4	0.3%
SSL	2	0.2%	2	0.5%	4	0.3%
CISA	3	0.3%	-	0.0%	3	0.2%
IMPI	2	0.2%	1	0.2%	3	0.2%
ISO/IEC 31000	2	0.2%	1	0.2%	3	0.2%
MAAGTIC	-	0.0%	3	0.7%	3	0.2%
Normas de la CNBV	2	0.2%	1	0.2%	3	0.2%
pmbook	1	0.1%	2	0.5%	3	0.2%
Otros	45	4.1%	42	10.3%	87	5.7%

Se observa que un 26.7% de los No-Informáticos reconoció e hizo mención de al menos un elemento normativo enfocado a la Seguridad de la Información, número significativamente más alto que en el estudio anterior, en donde sólo el 17.7% de este grupo reflejó este hallazgo. Es un crecimiento de 9.0%, si bien cabe considerar que 4.3% de los entrevistados No-Informáticos mencionaron alguna guía de normas o políticas internas de su organización y 22.4% de algún estándar o norma convencional. La tendencia se vuelve mucho más relevante, si se considera que en 2008 únicamente el 6.8% de entrevistados de este grupo, mencionó conocer alguna reglamentación sobre el tema.



GRÁFICA 8 – NORMAS Y REGULACIONES QUE CONOCE

En el grupo de los Informáticos, el número de entrevistados que mencionó algún estándar o norma enfocado a la seguridad de la información, disminuyó de un 54.0% registrado en el estudio anterior a sólo un 41.4% Llama la atención este hecho, en un año en que la publicación de la nueva ley sobre Protección de Datos Personales está muy fresca, la cual fue mencionada únicamente por el 0.5% de entrevistados de este grupo.

Qué hace falta por parte de los proveedores de TI

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

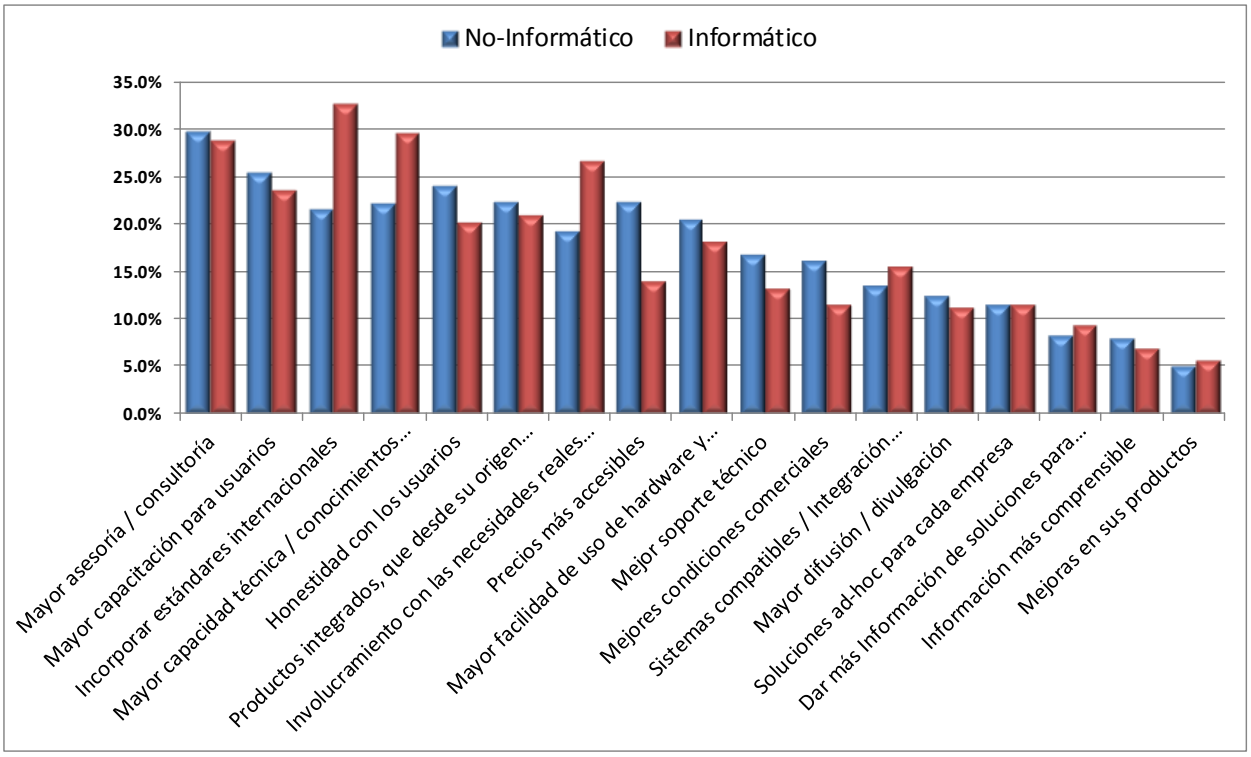
La tabla de frecuencias y gráfica de respuestas a esta pregunta se presentan, respectivamente, en la Tabla 5 y en la Gráfica 9.

TABLA 5

	No-Informáti		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Mayor asesoría / consultoría	330	29.8%	117	28.8%	447	29.5%
Mayor capacitación para usuarios	282	25.5%	96	23.6%	378	25.0%
Incorporar estándares internacionales	240	21.7%	133	32.8%	373	24.6%
Mayor capacidad técnica / conocimientos de los provee	246	22.2%	120	29.6%	366	24.2%
Honestidad con los usuarios	267	24.1%	82	20.2%	349	23.1%
Productos integrados, que desde su origen sean seguro	247	22.3%	85	20.9%	332	21.9%
Involucramiento con las necesidades reales del cliente	213	19.2%	108	26.6%	321	21.2%
Precios más accesibles	248	22.4%	57	14.0%	305	20.1%
Mayor facilidad de uso de hardware y software	227	20.5%	74	18.2%	301	19.9%
Mejor soporte técnico	186	16.8%	54	13.3%	240	15.9%
Mejores condiciones comerciales	180	16.2%	47	11.6%	227	15.0%
Sistemas compatibles / Integración multimarcas	151	13.6%	63	15.5%	214	14.1%
Mayor difusión / divulgación	139	12.5%	46	11.3%	185	12.2%
Soluciones ad-hoc para cada empresa	129	11.6%	47	11.6%	176	11.6%
Dar más Información de soluciones para PyME	93	8.4%	38	9.4%	131	8.7%
Información más comprensible	89	8.0%	28	6.9%	117	7.7%
Mejoras en sus productos	57	5.1%	23	5.7%	80	5.3%

De manera muy similar a los resultados de 2009, de acuerdo a la percepción de los Informáticos la principal exigencia hacia los proveedores de tecnología es la **incorporación de estándares internacionales** a sus servicios o productos (32.8% de los entrevistados de este grupo). Con un nivel menor de menciones, pero con bastante peso aún, los Informáticos demandan una **mayor capacidad técnica y conocimiento** por parte de los proveedores, así como una mayor **asesoría / consultoría** e **involucramiento con las necesidades reales de sus clientes.**

Es claro que los usuarios No-Informáticos demandan de los proveedores de tecnología una **mayor asesoría / consultoría**, en primer lugar, seguida de una **mayor capacitación** por parte del proveedor hacia ellos, **honestidad con los usuarios** y **precios más accesibles**, principalmente.



GRÁFICA 9 – QUÉ HACE FALTA POR PARTE DE LOS PROVEEDORES DE TI

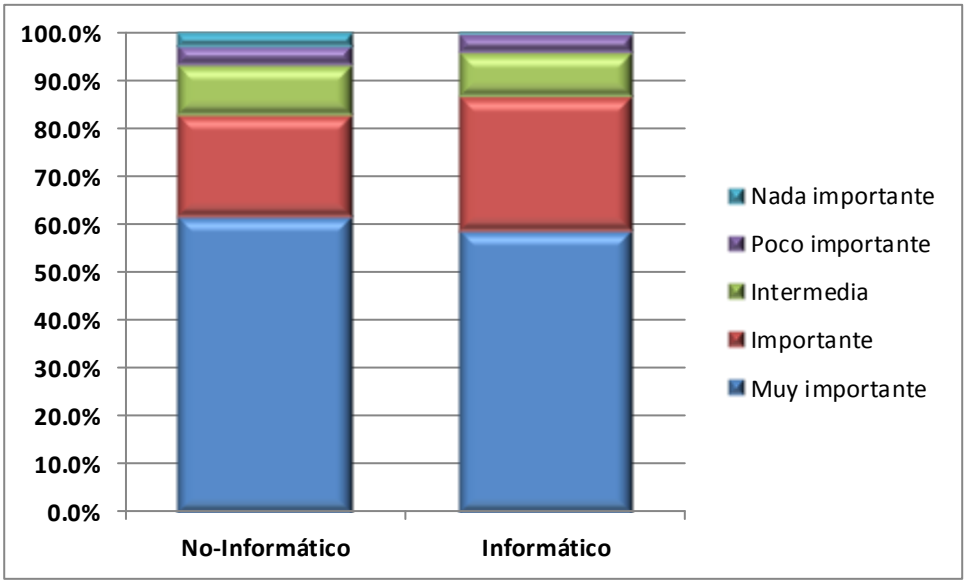
Importancia de la Seguridad en Informática en las empresas

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

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

En general, comparativamente con el estudio anterior, creció ligeramente la percepción **negativa** sobre este tema (5.9% este año vs. 3.7% de menciones de ambos grupos en conjunto, que afirman que la Seguridad de la Información tiende a ser “poco importante” o “nada importante”).

Aun así la mayoría de los entrevistados, tanto No-Informáticos como Informáticos, tienen una percepción positiva acerca de las organizaciones donde laboran, respecto a la importancia que sus directivos dan a la Seguridad de la Información. Del grupo de los usuarios No-Informáticos, 83.0% opina que la Seguridad de la Información tiene una importancia marcada para sus organizaciones (61.7% Muy importante y 21.3 Importante), mientras que un 86.7 de los Informáticos, aunque en diferente proporción, tiene esta misma percepción (58.9% Muy importante y 27.8 importante). Para el primer grupo, sólo 6.5% de los entrevistados considera que la Seguridad de la información es poco importante o nada importante dentro de las organizaciones donde laboran, mientras que para los Informáticos esta cifra es menor (4.2%).



GRÁFICA 10 – IMPORTANCIA DE LA SEGURIDAD EN INFORMÁTICA EN LAS EMPRESAS

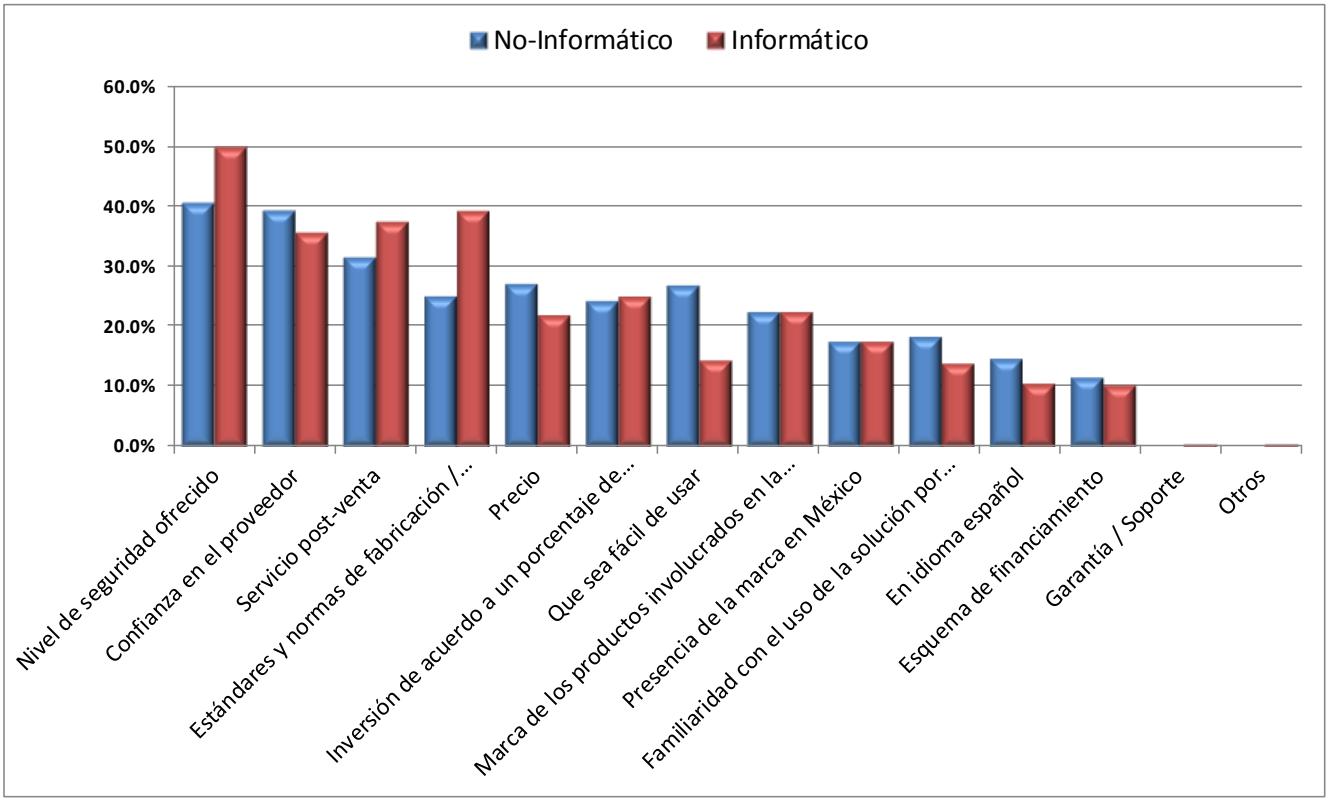
Aspectos a tomar en cuenta en la compra de tecnología

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

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

TABLA 6

	No-Informáti		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Nivel de seguridad ofrecido	451	40.7%	203	50.0%	654	43.2%
Confianza en el proveedor	436	39.4%	145	35.7%	581	38.4%
Servicio post-venta	348	31.4%	152	37.4%	500	33.0%
Estándares y normas de fabricación / integración	279	25.2%	160	39.4%	439	29.0%
Precio	300	27.1%	89	21.9%	389	25.7%
Inversión de acuerdo a un porcentaje de los ingresos d	270	24.4%	102	25.1%	372	24.6%
Que sea fácil de usar	297	26.8%	59	14.5%	356	23.5%
Marca de los productos involucrados en la solución	249	22.5%	91	22.4%	340	22.5%
Presencia de la marca en México	196	17.7%	71	17.5%	267	17.6%
Familiaridad con el uso de la solución por parte de los e	202	18.2%	57	14.0%	259	17.1%
En idioma español	162	14.6%	43	10.6%	205	13.5%
Esquema de financiamiento	130	11.7%	42	10.3%	172	11.4%
Garantía / Soporte	3	0.3%	2	0.5%	5	0.3%
Otros	1	0.1%	2	0.5%	3	0.2%



GRÁFICA 11 – ASPECTOS A TOMAR EN CUENTA EN LA COMPRA DE TECNOLOGÍA

A diferencia del estudio realizado en 2009, en esta ocasión el Nivel de Seguridad ofrecido por las soluciones tecnológicas es el rubro más importante, tanto para informáticos como para No-Informáticos, cuando en el estudio anterior el Precio había sido el factor considerado en primera instancia por el grupo de No-Informáticos.

Para los usuarios No-informáticos, el segundo factor de mayor peso a considerar en la compra de tecnología, es la **Confianza en el proveedor** (39.4%), seguido del **Servicio post-venta** (31.4), el Precio (27.1%) y la **Facilidad de uso** de los productos (26.8%).

Para el grupo de los usuarios Informáticos, después del **Nivel de seguridad ofrecido**, con un 50.0%, está la inclusión de **Estándares y normas de fabricación** (para un 39.4% de los entrevistados), seguida por **Servicio post-venta** (con un 37.4%) y **Confianza en el proveedor** (35.7% de menciones).

Sobresale el hecho de que para los Informáticos, el **Precio** adquirió menor importancia, ya que fue mencionado por tan sólo un 21.9% de este grupo de entrevistados, mientras en el estudio anterior estas menciones fueron expresadas por un 30.8%

Percepción acerca de diversas marcas asociadas con Seguridad en Informática

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

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

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

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

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

TABLA 7

	No-Informático		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Norton / Symantec	230	20.8%	88	21.7%	318	21.0%
Cisco	129	11.6%	86	21.2%	215	14.2%
McAfee	131	11.8%	56	13.8%	187	12.4%
Apple / Mac	99	8.9%	38	9.4%	137	9.0%
HP	94	8.5%	37	9.1%	131	8.7%
Kaspersky	54	4.9%	32	7.9%	86	5.7%
Dell	59	5.3%	15	3.7%	74	4.9%
Eset / Nod32	49	4.4%	20	4.9%	69	4.6%
Juniper	40	3.6%	25	6.2%	65	4.3%
Panda	51	4.6%	14	3.4%	65	4.3%
Check Point	40	3.6%	23	5.7%	63	4.2%
Trend Micro / PC Cillin	30	2.7%	32	7.9%	62	4.1%
Microsoft	39	3.5%	13	3.2%	52	3.4%
IBM	30	2.7%	18	4.4%	48	3.2%
AVG	34	3.1%	11	2.7%	45	3.0%
Linux	31	2.8%	8	2.0%	39	2.6%
Nokia	28	2.5%	8	2.0%	36	2.4%
Sony	27	2.4%	5	1.2%	32	2.1%
Avast	21	1.9%	10	2.5%	31	2.0%
3Com / Tipping Point	16	1.4%	13	3.2%	29	1.9%
Fortinet	13	1.2%	16	3.9%	29	1.9%
Sun / Solaris	18	1.6%	10	2.5%	28	1.8%
Windows	12	1.1%	11	2.7%	23	1.5%
Nortel	14	1.3%	8	2.0%	22	1.5%
Oracle	11	1.0%	8	2.0%	19	1.3%
Verisign	11	1.0%	6	1.5%	17	1.1%
Websense	6	0.5%	10	2.5%	16	1.1%
Panasonic	11	1.0%	3	0.7%	14	0.9%
Toshiba	11	1.0%	3	0.7%	14	0.9%
Barracuda	4	0.4%	9	2.2%	13	0.9%
Compaq	10	0.9%	2	0.5%	12	0.8%
Acer	10	0.9%	1	0.2%	11	0.7%
RSA	6	0.5%	5	1.2%	11	0.7%
EMC	4	0.4%	6	1.5%	10	0.7%
Linksys	5	0.5%	5	1.2%	10	0.7%
Ad-aware	6	0.5%	3	0.7%	9	0.6%
AMD	4	0.4%	4	1.0%	8	0.5%
Intel	6	0.5%	2	0.5%	8	0.5%
Internet Explorer	2	0.2%	5	1.2%	7	0.5%
Novell	5	0.5%	2	0.5%	7	0.5%
BitDefender	4	0.4%	2	0.5%	6	0.4%
Stonesoft	5	0.5%	1	0.2%	6	0.4%
Unix	4	0.4%	2	0.5%	6	0.4%
Avaya	5	0.5%	0	0.0%	5	0.3%
Avira	4	0.4%	1	0.2%	5	0.3%
Blue Coat	2	0.2%	3	0.7%	5	0.3%
Citrix	2	0.2%	3	0.7%	5	0.3%
Guardium	5	0.5%	0	0.0%	5	0.3%
ISS	3	0.3%	2	0.5%	5	0.3%
Lanix	1	0.1%	4	1.0%	5	0.3%
Samsung	1	0.1%	4	1.0%	5	0.3%
CA	3	0.3%	1	0.2%	4	0.3%
Forefront	1	0.1%	3	0.7%	4	0.3%
SafeNet	3	0.3%	1	0.2%	4	0.3%
Software libre (Sin especificar)	4	0.4%	0	0.0%	4	0.3%
VeriZone	4	0.4%	0	0.0%	4	0.3%
Benq	2	0.2%	2	0.5%	4	0.3%
Otros	125	11.3%	70	17.2%	195	12.9%

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

TABLA 8

	No-Informático		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Norton / Symantec	156	14.1%	97	23.9%	253	16.7%
McAfee	59	5.3%	59	14.5%	118	7.8%
Panda	76	6.9%	32	7.9%	108	7.1%
Microsoft	53	4.8%	40	9.9%	93	6.1%
Windows	41	3.7%	21	5.2%	62	4.1%
AVG	43	3.9%	12	3.0%	55	3.6%
Dell	19	1.7%	12	3.0%	31	2.0%
Toshiba	15	1.4%	11	2.7%	26	1.7%
Trend Micro / PC Cillin	12	1.1%	11	2.7%	23	1.5%
Acer	12	1.1%	9	2.2%	21	1.4%
HP	12	1.1%	7	1.7%	19	1.3%
Cisco	8	0.7%	8	2.0%	16	1.1%
Eset / Nod32	5	0.5%	10	2.5%	15	1.0%
IBM	7	0.6%	8	2.0%	15	1.0%
Nortel	14	1.3%	0	0.0%	14	0.9%
Apple / Mac	7	0.6%	4	1.0%	11	0.7%
Avira	9	0.8%	2	0.5%	11	0.7%
Sony	9	0.8%	2	0.5%	11	0.7%
Compaq	6	0.5%	4	1.0%	10	0.7%
Fortinet	5	0.5%	5	1.2%	10	0.7%
Linux	7	0.6%	3	0.7%	10	0.7%
3Com / Tipping Point	5	0.5%	3	0.7%	8	0.5%
Avast	7	0.6%	1	0.2%	8	0.5%
Hauri	7	0.6%	1	0.2%	8	0.5%
Productos sin marca	5	0.5%	3	0.7%	8	0.5%
Freeware / Shareware	4	0.4%	3	0.7%	7	0.5%
Intel	3	0.3%	4	1.0%	7	0.5%
Internet Explorer	6	0.5%	1	0.2%	7	0.5%
Juniper	5	0.5%	2	0.5%	7	0.5%
Kaspersky	4	0.4%	3	0.7%	7	0.5%
Lanix	4	0.4%	3	0.7%	7	0.5%
Linksys	2	0.2%	5	1.2%	7	0.5%
Samsung	3	0.3%	4	1.0%	7	0.5%
Benq	3	0.3%	3	0.7%	6	0.4%
Software pirata	3	0.3%	3	0.7%	6	0.4%
Prodigy	4	0.4%	1	0.2%	5	0.3%
Sonicwall	1	0.1%	4	1.0%	5	0.3%
AMD	3	0.3%	1	0.2%	4	0.3%
Barracuda	1	0.1%	3	0.7%	4	0.3%
BMC	2	0.2%	2	0.5%	4	0.3%
Forefront	-	0.0%	4	1.0%	4	0.3%
Otros	56	5.1%	19	4.7%	75	5.0%

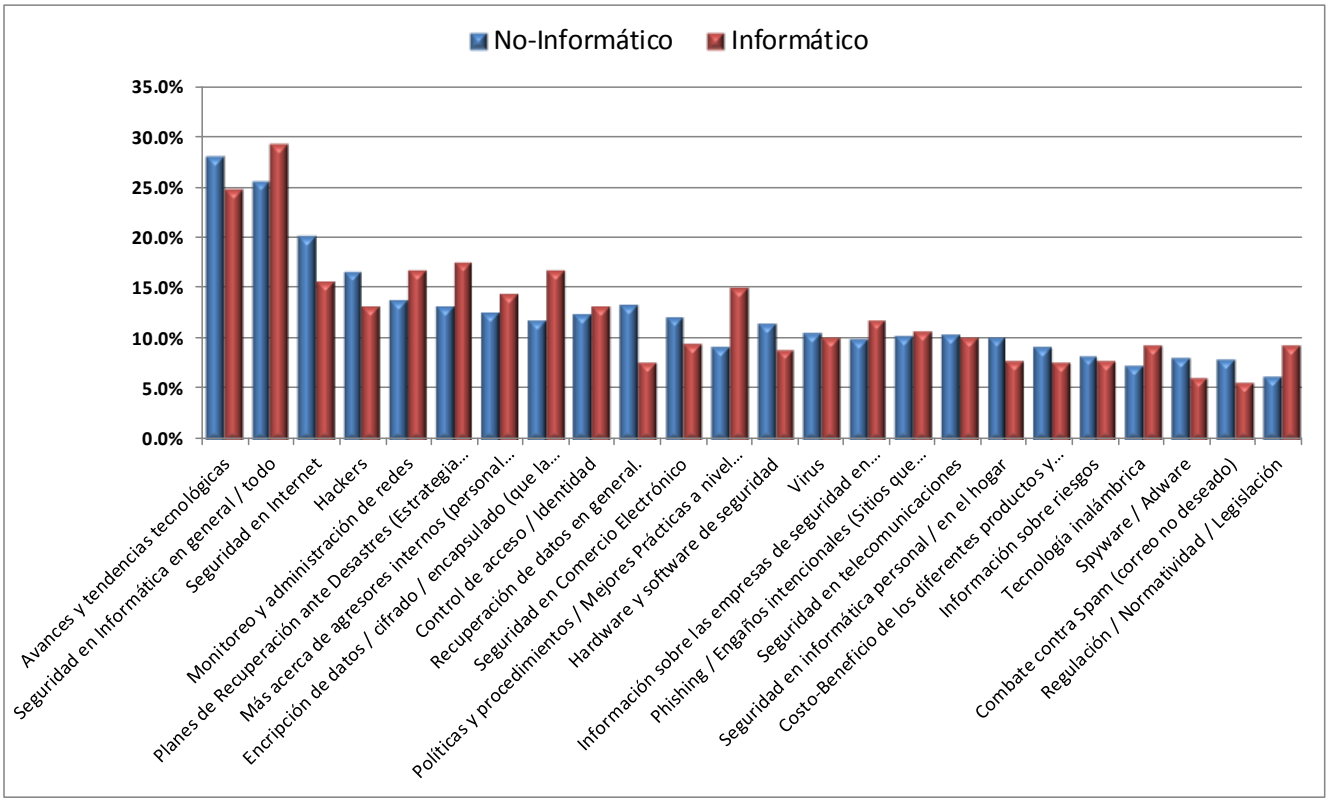
Qué más les gustaría conocer acerca de Seguridad en Informática

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

Ver tabla de frecuencias de la muestra total (Tabla 9) y Gráfica 12, así como comparativo entre Informáticos y No-Informáticos, ordenado en orden de importancia para cada grupo (Tabla 10).

	No-Informáti		Informático		Total	
Muestra:	**1108**		**406**		**1,514**	
Avances y tendencias tecnológicas	311	28.1%	101	24.9%	412	27.2%
Seguridad en Informática en general / todo	284	25.6%	119	29.3%	403	26.6%
Seguridad en Internet	224	20.2%	64	15.8%	288	19.0%
Hackers	184	16.6%	54	13.3%	238	15.7%
Monitoreo y administración de redes	154	13.9%	68	16.7%	222	14.7%
Planes de Recuperación ante Desastres (Estrategia qu	147	13.3%	71	17.5%	218	14.4%
Más acerca de agresores internos (personal malintenci	140	12.6%	59	14.5%	199	13.1%
Encripción de datos / cifrado / encapsulado (que la infor	131	11.8%	68	16.7%	199	13.1%
Control de acceso / Identidad	138	12.5%	54	13.3%	192	12.7%
Recuperación de datos en general.	149	13.4%	31	7.6%	180	11.9%
Seguridad en Comercio Electrónico	135	12.2%	39	9.6%	174	11.5%
Políticas y procedimientos / Mejores Prácticas a nivel m	103	9.3%	61	15.0%	164	10.8%
Hardware y software de seguridad	128	11.6%	36	8.9%	164	10.8%
Virus	118	10.6%	41	10.1%	159	10.5%
Información sobre las empresas de seguridad en inform	110	9.9%	48	11.8%	158	10.4%
Phishing / Engaños intencionales (Sitios que aparentan	114	10.3%	44	10.8%	158	10.4%
Seguridad en telecomunicaciones	116	10.5%	41	10.1%	157	10.4%
Seguridad en informática personal / en el hogar	113	10.2%	32	7.9%	145	9.6%
Costo-Beneficio de los diferentes productos y servicios	103	9.3%	31	7.6%	134	8.9%
Información sobre riesgos	92	8.3%	32	7.9%	124	8.2%
Tecnología inalámbrica	82	7.4%	38	9.4%	120	7.9%
Spyware / Adware	90	8.1%	25	6.2%	115	7.6%
Combate contra Spam (correo no deseado)	88	7.9%	23	5.7%	111	7.3%
Regulación / Normatividad / Legislación	70	6.3%	38	9.4%	108	7.1%

TABLA 9 – QUÉ MÁS QUISIERA CONOCER SOBRE EL TEMA



GRÁFICA 12 – QUÉ MÁS QUISIERA CONOCER SOBRE EL TEMA

Las prioridades de conocimiento para los Informáticos fueron, en orden de importancia, temas en general sobre Seguridad en Informática, Avances y Tendencias Tecnológicas, Planes de Recuperación ante Desastres, Monitoreo y Administración de Redes.

Para los No-Informáticos, aunque comparten inquietudes similares, sus prioridades cambian y giran alrededor de Avances y Tendencias Tecnológicas, Seguridad en Informática en general, Seguridad en Internet, Hackers, Monitoreo y Administración de Redes, así como Recuperación de Datos en general.

Vuelve a llamar la atención, al igual que en años anteriores, que los temas sobre Regulación, Normatividad y Legislación, permanecen en los últimos lugares (último en esta ocasión) del interés de conocimiento de los entrevistados.

Principales diferencias entre No-Informáticos e Informáticos

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

TABLA 10

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

La diferencia más significativa entre ambos grupos (No-Informáticos e Informáticos), se da alrededor del concepto de “Recuperación de datos en general” (mencionada en el lugar 10 y 21 respectivamente). Esta percepción diferenciada, podría indicar que el grupo de No-Informáticos tiende a pensar en mecanismos más correctivos que preventivos, frente a los Informáticos, o bien que el primer grupo tiene un mayor desconocimiento sobre el tema y por lo mismo le representa una preocupación de más peso.

Es claro que para ambos grupos, el combate contra el Spam no es un rubro de interés, respecto de los otros temas mencionados.

Respecto de los resultados del estudio anterior, llaman la atención los siguientes hallazgos:

No-Informáticos	Informáticos
Este grupo de entrevistados muestra este año un mayor interés por el tema de **Políticas, Procedimientos y Mejores Prácticas**, ubicándose en la posición 12, mientras en el estudio anterior fue la mención número 22.	El tema de **Regulación, Normatividad y Legislación**, tiene ahora una posición más importante en el interés de este grupo, habiendo subido de la mención 23 a la 17, aunque sigue siendo de los rubros más bajos..
De manera similar al estudio anterior, es notoria una falta de interés por parte de este grupo, acerca de aspectos de **Regulación, Normatividad y Legislación**, en relación con los otros temas.	

III. ESTUDIO CON EXPERTOS Y PROVEEDORES LÍDERES DEL MERCADO TI

Objetivos del estudio

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

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

Metodología

Método de investigación

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

Relación de entrevistados

Empresa	Nombre	Puesto
ALAPSI	Raúl Aguirre	Director de TI y Dirección de Educación
CommIT Service Management, S.A. de C.V.	Nicolás Lara González	Socio-Director
Factory Tec, S.A. de C.V.	Raúl Aguirre García	Consultor
Grupo Corporativo Diamante	Jose Luis Rojo y Arabi	Presidente

Instituto Federal de Acceso a la Información y Protección de Datos	Guillermo Preciado López	Director de Informática
Integridata	Erik Zepeda Peralta	Arquitecto IT
Metronet	Jorge Garibay Orozco	CIO (Director de Tecnología de Información y Comunicaciones)
Sentrigo	Oriana Weber	Preventa Alemania
Sector financiero (sin especificar)	Anónimo (Por solicitud expresa del respondente)	Especialista en Seguridad Informática

Resultados

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

El rango de respuestas varió mucho, desde quienes ven un panorama negativo que requiere acciones urgentes, hasta otros que opinan que la situación de México es la adecuada, pasando por varios que hicieron notar algunos rubros en los que tenemos ventaja como país y otros en los que hay que esforzarse para mejorar. Esto es interesante en sí mismo, al no haber un consenso claro entre los diversos respondentes.

Principales progresos

Se reconoce que existen ciertos avances que colocan a nuestro país, incluso, por encima de otros, tanto de Europa como de América Latina. Tal es el caso de algunos eventos aislados, como los siguientes:

- A nivel infraestructura, se observa que las grandes empresas y las mayores instituciones gubernamentales, pueden contar con todo lo necesario para lograr altos esquemas de seguridad.
- Aunque no son muchos, existe un buen número de profesionales debidamente capacitados en el tema, con las certificaciones necesarias para cubrir aspectos de seguridad en diversos ámbitos y especialidades.
- En materia legislativa, ya se cuenta con una Ley de Protección de Datos Personales que, si bien sólo cubre una parte del amplio espectro de necesidades de seguridad, se puede considerar como un buen inicio.

Principales rezagos

Se percibe que a pesar de algunos aspectos positivos y avances en materia de Seguridad de la Información en nuestro país, existen rezagos que, en conjunto, colocan a México como un país con mayores carencias que progresos. Entre ellas:

- Pese a los avances legislativos observados con la publicación de la Ley de Protección de Datos Personales en Posesión de Particulares, se considera que no existen directrices claras que definan las consecuencias que podrían darse en caso de incumplimiento. Además, existen muchos otros aspectos sobre los cuales es necesario tener una regulación adecuada.
- La mayoría de las organizaciones en México, pertenecen al segmento PyME y de microempresas. En ellas no se siguen prácticas ni se tienen infraestructuras robustas de seguridad, lo cual coloca los recursos (tanto de empresas privadas como de instituciones públicas) en una posición altamente vulnerable.
- A nivel educativo se perciben también rezagos importantes. La cantidad de personas de todas las edades que se están incorporando al uso de Internet en México, es muy elevado. Las instituciones educativas y maestros comparten su preocupación por que sus alumnos estén a la vanguardia de la tecnología y las comunicaciones, pero en materia de seguridad proporcionan "indicaciones mínimas o nulas de cómo auto-protegerse de pornografía, depredadores sexuales, sectas y otras amenazas que llevan muchos años perfeccionando sus técnicas".
- Se percibe que aún no se tiene la madurez suficiente en el país, para construir una cultura de colaboración organizacional. No existe una verdadera coordinación entre las diversas instituciones y sectores, para lograr que los esfuerzos que se realizan por tener una mayor seguridad.
- Asimismo, se tiene la percepción de que seguimos haciendo adaptaciones de estrategias foráneas, para tratar de que funcionen en nuestra realidad, cuando deberíamos empezar a crearlas en función de nuestro entorno y particularidades.

PRINCIPALES OBSERVACIONES

"México es uno de los países con el mayor crecimiento en adopción de uso de internet, sin embargo, no se tienen las medidas de seguridad necesarias para hacer que la entrada a estas tecnologías sea de manera segura".

"Salvo las instituciones financieras y algunas dependencias de gobierno, no se nota una cultura robusta en temas de seguridad de la información".

"En las preparatorias y carreras profesionales ocurren plagios, exposición de datos personales, acosos y otros males, por la misma carencia de educación. En algunos países en el llamado primer mundo, se aprovecha la tecnología pero se cuida a los usuarios, por ejemplo en Inglaterra ya hay un

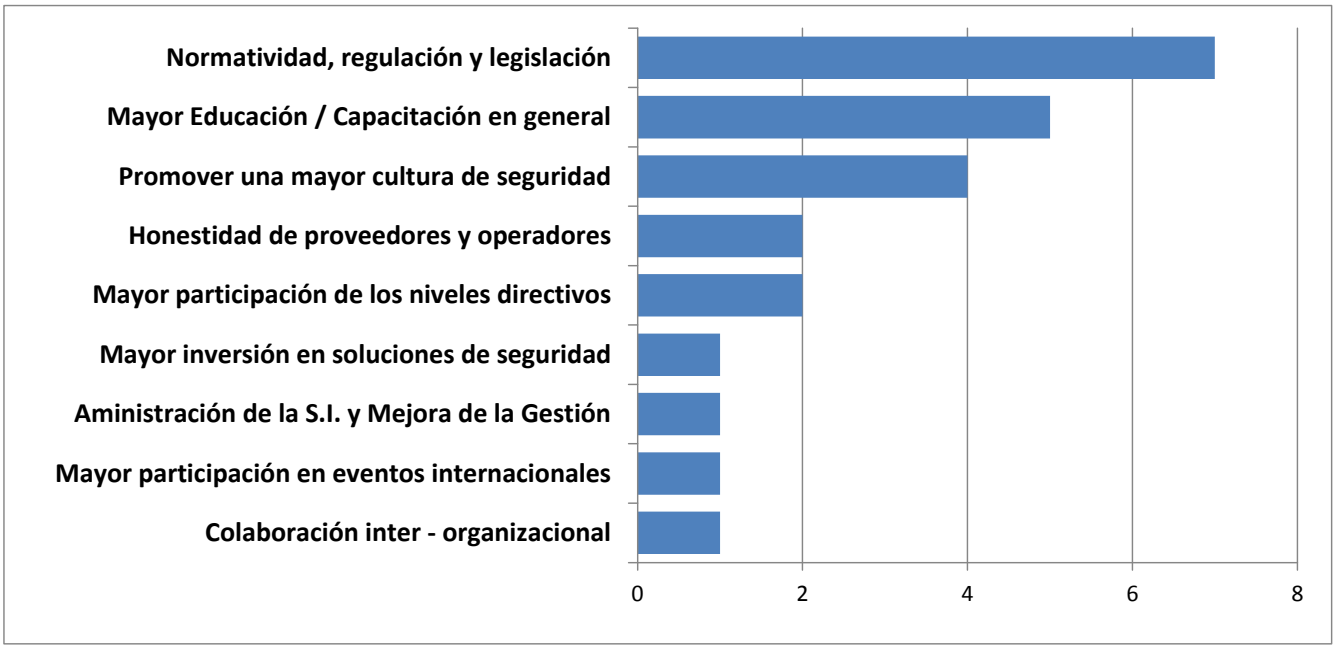
*programa de **"red button"** en el que un niño o joven que se sienta agredido en Internet puede hacer uso de este recurso y las autoridades inician una investigación de quién es el atacante en la red".*

"Han surgido certificaciones de todo tipo de especialidades en seguridad; sin embargo aún no hay una que cubra necesidades específicas del país. Por ejemplo, una queja constante es: por qué usar estándares que parecieran haber sido hechos para empresas enormes, si en nuestro país más del 80% son pequeñas o medianas empresas. Por qué estudiar legislación de otros países en lugar de tratar de generar legislación informática en nuestro país. Por qué toda la literatura está en Inglés, Francés, Portugués, Chino etc. Por qué no hay suficientes normas y mejores prácticas de seguridad nacionales, etc. etc. En resumen falta una adecuación de programas de certificación, de carreras universitarias y posgrados, orientados a la realidad del país".

"Hace falta una cultura de cooperación organizacional, México está a la vanguardia en infraestructura tecnológica en comparación con muchos países de Europa, pero lo que nos frena para avanzar es que nos hace falta trabajar en conjunto entre varias entidades para lograr objetivos comunes y atacar problemas comunes. Ésa es la gran diferencia: el factor humano y la cultura individualista que no nos ayuda".

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

Las respuestas codificadas de todos los entrevistados giraron alrededor de nueve rubros principalmente, como puede observarse en la Gráfica 13.



GRÁFICA 13

A pesar de que en los últimos 2 años se han dado hallazgos importantes en materia legislativa y de normatividad (como consecuencia de la publicación de leyes alrededor de la protección de datos personales), la mayoría de los expertos entrevistados considera que uno de los retos más importantes sigue siendo la parte regulatoria. Los avances que se van dando, no son lo suficientemente rápidos, como lo es la incorporación de la tecnología y los cambios tan acelerados que se dan en los hábitos y costumbres de las personas y las organizaciones, en materia de comunicación y colaboración.

En el terreno educativo se sigue considerando que los esfuerzos son incipientes. El ámbito se limita a la formación de especialidades o a la organización de escasos seminarios. Sin embargo los temas de Seguridad de la Información deberían ser, además de un pilar fundamental en todas las carreras de sistemas o de informática a nivel nacional, materia de los programas de educación primaria y media e inclusive promover su difusión en el hogar, la escuela y otros centros de participación social.

PRINCIPALES OBSERVACIONES

"Debiera ser una materia obligatoria en todas los planes curriculares de estudio".

"Debe hacerse conscientes a los dueños de los negocios tomadores de decisión".

"Utilizar la infraestructura existente para trabajar en equipo con todas las entidades existentes que se ocupan del tema. Seguramente hay más de una organización o entidad que se ocupa en esta materia; el gran problema es que en México no tenemos ese espíritu de colaboración donde la información y los recursos se comparten para beneficio del país".

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

Entre los retos que fueron considerados como más relevantes para ser considerados por este tipo de organizaciones, se mencionaron los siguientes:

- Crear esquemas robustos de seguridad, contando con profesionales en la materia o con compañías especializadas que les provean ese servicio, considerando que la propiedad de los planes de seguridad es de la empresa y NO del *outsourcer*.

- Las regulaciones son el motor imperativo principal. Hay varias y cada vez más regulaciones, que están siendo el camino para lograr la protección y la seguridad de las empresas (proveedores y clientes) y de las personas en general.

- Concientización, para al menos usar la tecnología de manera que no se exponga ni al individuo ni a su empresa.

- Regulaciones y cumplimiento, Robo de identidad, BCP y DRP, Spam, Malware

- Los dueños deben tener la iniciativa, los incentivos de valor y de supervivencia para activar su programa de protección de la información. Deben capacitarse junto con su personal con programas prácticos de protección de la información.

- Ética, Capacitación, definición de roles y políticas de seguridad (qué es lo que hay que proteger, quién hace qué, quién controla qué o a quién)

- Tomar conciencia de la importancia de la seguridad de IT y hacer algo para mejorar día con día. Alinear las estrategias de seguridad de la información con las estrategias del negocio o institución.

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

Los entrevistados opinan que los proveedores deben difundir una cultura de seguridad que haga conciencia en los usuarios de sus tecnologías y fomente la participación de soluciones robustas que apoyen al negocio en la consecución de sus objetivos, sin sacrificar la integridad, confidencialidad y disponibilidad de la información.

Se considera que en este sentido existen 2 ámbitos de responsabilidad, los fabricantes por un lado y los distribuidores por el otro. Los fabricantes deben integrar medidas tendientes a la movilidad segura con soluciones flexibles de fábrica; los Distribuidores, Canales y Consultores/Asesores, deben de alinearse con sus servicios de acuerdo a las necesidades de cada institución. “A la medida es el término antiguo acuñado, que sigue ahora siendo mandatorio”. En ambos casos, que se tengan controles de seguridad en todo el ciclo de vida de desarrollo de sus productos.

PRINCIPALES OBSERVACIONES

“La experiencia dice que más del 40% de los errores que se introducen en los productos se hace desde la fase del diseño de los mismos”

“Seguridad en aplicaciones, Control de acceso, Criptografía, Seguridad en Redes (virus, malware, etc.)”.

“Hacer bien las cosas, metodologías adecuadas y vigilar que se hagan bien”.

"Ética, vanguardia, apego a las leyes, seguridad física".

"Buscar soluciones prácticas y ofrecerlas en proyectos integrales".

"Identificar las soluciones tecnológicas idóneas para el mercado nacional".

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

Una vez más, los entrevistados coinciden en que se deben crear planes de estudio que consideren a la seguridad informática como parte de sus descripciones curriculares, impulsando la formación de más profesionales en la materia. Esto significa profesionalizar desde el inicio, hasta la preparación académica en diferentes niveles (conferencias, pláticas, cursos, talleres, diplomados, certificaciones, especializaciones, maestrías, doctorados).

Se considera asimismo urgente, la incorporación de programas educativos completos que contemplen la capacitación profunda y adecuada tanto de los instructores como de los alumnos, en el uso seguro de sus equipos. Esto puede ser instrumentado tanto a través de libros, como de folletos y algunos otros recursos de apoyo.

Otro reto importante para este sector, consiste en la inversión de recursos. Deben conseguirse alianzas, subsidios o financiamientos para que la infraestructura de TIC de la educación en México cuente con controles de seguridad básicos como antivirus, protectores de navegación, etc.

PRINCIPALES OBSERVACIONES

"Éntre los principales retos, están la ética, seguridad física, capacitación, vanguardia, conocimiento de las leyes locales, nacionales e internacionales aplicables."

"Incrementar la cultura en seguridad informática y control de Internet de los estudiantes que la usan como medios de proselitismo antisocial".

"Formar profesionales con especialización en seguridad IT".

"Orientar la currícula hacia la formación de profesionales con visión estratégica en materia de seguridad informática".

"Que se hagan las inversiones necesaria en todas las escuelas y se eduque en la preparación y cultura de la investigación, autoestudio y aprendizaje virtual y semivirtual; sin descuidar los círculos de verificación y certificación, de aplicación y de intercambio".

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

PRINCIPALES OBSERVACIONES
"Difundir no sólo las nuevas tendencias tecnológicas, sino hacer énfasis en el uso seguro de ellas y los riesgos a los que se exponen si no cuentan con las medidas de seguridad apropiadas".
"Que se difunda la normatividad en lo general (leyes, regulaciones, reglamentos, circulares) y la normatividad interna de cada institución orientada a cada audiencia, para ser prácticos y no saturar con indicaciones inútiles y nada prácticas. En toda institución, contar con un programa adecuado de Concienciación y capacitación sobre la Seguridad en la Información y de la Auditoría en Informática (programas, noticias, …)".
"Invertir en seguridad para garantizar al menos integridad, confidencialidad y disponibilidad de los medios de comunicación, que ofrecen a sus usuarios".
"Regulaciones y cumplimiento, Seguridad móvil, Firmas de seguridad".
"Ética, capacitación, conocimiento de las leyes locales, nacionales e internacionales aplicables, seguridad física".
"Difundir por este medio las alertas de ataques a los medios de seguridad y realizar recomendaciones en general para los usuarios de los medios cibernéticos".
"Tener segmentos dedicados a la difusión y concientización".
"Transparentar las noticias referentes al tema y evitar el amarillismo y la deformación de los hechos".

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

Entre los principales retos mencionados por los entrevistados, están:

- Crear foros permanentes de difusión y adopción de estándares internaciones, así como la creación de las legislaciones necesarias que fortalezcan los temas de la seguridad de la información.

- Estandarización de servicios, de procesos y de productos, e implementación de sistemas de gestión de la seguridad de la información e inclusión de la práctica de auditoría en informática, alineados las necesidades de cada Institución.

- *"Si bien se han emitido normas para unificar criterios de gobernabilidad y de controles de seguridad, son de reciente creación. Los QUÉS están puestos en la mesa, ahora es necesario que asociaciones sin fines de lucro asesoren al gobierno para aterrizar a la realidad del país los CÓMOS. Creo que si no se organiza una estrategia nacional en el gobierno, esto puede conducir a un caos, con beneficios de algunos pocos y sin necesariamente lograr el objetivo de hacer un gobierno (electrónico) más efectivo y eficiente para los contribuyentes".*

PRINCIPALES OBSERVACIONES

"Apoyar en programas de adecuación a las necesidades propias de nuestra localidad, estado o país".

"Fomentar la certificación del usuario seguro".

"Fomentar la certificación del maestro que enseña a sus alumnos a tener prácticas de seguridad en la información; y la certificación del alumno por sus avances".

"En las escuelas poner guías de protección o reacción a los ataques de Ciberbullying, u otros semejantes que son difíciles de controlar, tanto para directores de escuela, sicólogos, maestros, padres y para alumnos. Se hacen campañas de uso de los medios seguros para utilizar las computadoras en casa y educar a los hijos".

"Facilitar la integración, pero también el reconocimiento y la incentivación a colaborar a favor de la Asociación de personas que trabajen en grupos y en forma individual para aportar".

"Entre otros, están la ética, trabajo conjunto para lograr objetivos comunes, seguridad física, definición de roles y políticas de seguridad (qué es lo que hay que proteger, quién hace qué, quién controla qué o a quién)".

"Crear medidas de apremio, legislar y aplicar sanciones a quien por medio de los sistemas cibernéticos cause un daño a la economía o integridad de las personas, sin proteccionismo, ni impunidad".

"Ayudar en la creación de normas y reglamentos prácticos".

"De los principales retos, son el robo de identidad, Leyes, regulaciones y cumplimiento, Criptografía".

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

ALAPSI
Raúl Aguirre
Director de TI y Dirección de Educación

"Certificación y Consolidación de Servicios. A través de un Proveedor, canalizar todas las soluciones para que catalice e integre todos los requerimientos del servicio. Es un solo integrador frente a la institución o la empresa, buscando soluciones robustas y optimizadas para los procesos de la institución".

CommIT Service Management
Nicolás Lara González
Socio - Director

"Estamos adoptando políticas de seguridad en el uso de la información e infraestructura de TI, así como encriptación de computadoras móviles, uso de Appliances para combatir el Spam, virus, IPS, etc. En el desarrollo de aplicaciones se implantan medidas de seguridad para hacerlas más confiables".

Factory Tec
Raúl Aguirre García
Consultor

"Participamos en alianza con otras empresas que, asociadas con ALAPSI o AMIPCI, AMITI y otras, nos apoyamos para desarrollar soluciones rápidas y efectivas; sin embargo necesitamos un buen líder y apoyos económicos para ser más efectivos.

"Invito a propiciar un efecto acumulativo de información y modos de protegerse a través de recomendaciones y puntos de solución, por medio del portal del IFAI o de la Secretaría de Economía como entidades donde tenemos acceso todos a esto".

Grupo Corporativo Diamante
José Luis Rojo Arabi
Presidente

"Cursos sobre protección y seguridad informática".

Instituto Federal de Acceso a la Información y Protección de Datos
Guillermo Preciado López
Director de Informática

"La instrumentación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, mediante el desarrollo de los procesos, las aplicaciones y la capacitación sobre la materia".

Integridata
Erik Zepeda PERALTA
Arquitecto IT

"Vendemos cursos, promovemos la seguridad, ayudamos a las empresas a revisarla, implantarla, mejorarla, participamos en asociaciones como ALAPSI, nos capacitamos continuamente".

Institución financiera anónima
Especialista en Seguridad Informática

"La empresa en que laboro ha sido pionera en hacer sus propios desarrollos en el área de seguridad de la información, particularmente en criptografía, desde luego apoyado de empresas asesoras con la experiencia para este tipo de controles. Asimismo, considero una contribución que procure capacitar en materia de seguridad tanto en el ámbito nacional, como en el internacional, a las personas responsables de los sistemas que permiten cumplir con sus obligaciones como gobierno".

Metronet
Jorge Garibay Orozco
CIO (Director de Tecnología de Información y Comunicaciones)

"El uso de arquitecturas y medidas de seguridad para garantizar la operación confidencial y la integridad de la información no sólo de nuestra empresa, sino de las empresas a las cuales les brindamos algún servicio de tecnología".

Sentrigo
Oriana Weber
Preventa Alemania

"Difusión de un tema y tecnologías de vanguardia a nivel mundial: Seguridad y control de bases de datos".

IV. TEMA ESPECIAL DE LA EDICIÓN 2011: PROTECCIÓN DE DATOS PERSONALES

Implicación de la Protección de Datos Personales entre las organizaciones entrevistadas

Pregunta: En general, ¿qué importancia y en su caso qué implicaciones tiene la Protección de Datos Personales en el entorno particular de su organización?

Respuestas:

- Para nosotros es de uso obligatorio, ya que los servicios que prestamos a nuestros clientes son de operación y administración de la infraestructura de cómputo que soporta sus sistemas de información y en la mayoría de esto se encuentran bases de datos con información de personas. No tenemos opción de no cumplirla y creo que en este sentido es una Ley que apoya y protege a los usuarios finales que antes se encontraban muy vulnerables a la difusión de su información particular.

- Finalmente llegó la ley que desde hace muchos años se venía pidiendo se diera.

- Es de suma importancia, sin embargo, es más fácil decirlo que lograrlo.

- Es muy importante ya que el personal cuenta con información confidencial de nuestros clientes que al momento de quedar vulnerables tendría implicaciones legales para nuestra organización.

- Tiene una importancia desde varios enfoques:

    a. A modo personal, identificar qué actitudes se deben enriquecer para practicar el proteger la información privada, tanto mía, de mi familia, mis empleados, mis clientes y la de mis amigos. Tenemos que decidirnos a hacer algo, a apoyar.
    b. Aprender las diferentes actitudes de control para el mismo dato, pero que, dependiendo de las circunstancias, saber actuar con seguridad o con libertad y permiso para decir, publicar, utilizar los datos personales.
    c. Poner en práctica las indicaciones y las normas que deben traducirse en actitudes de todos los que trabajamos para la empresa y nuestros clientes.
    d. Identificar qué y cómo apoyar en la difusión de lo que se debe practicar.

- Es prioridad número uno, nuestras tecnologías tienen acceso directo a la información almacenada en las bases de datos, pero cuenta con los filtros necesarios para enviar alertas en caso de que alguna política de seguridad haya sido violada.

- Derivado de la delincuencia existente, donde es notable la forma, se ataca en diversos delitos a las personas y a la economía de éstas; la protección de los datos personales que se encuentra muy descuidada, se ha vuelto un generador y multiplicador de delitos.

- Es parte de nuestro negocio.

- Las implicaciones de este tema son trascendentales para nuestra organización, porque incrementan sustancialmente el alcance de las responsabilidades del IFAI, nuestra organización es la autoridad garante en materia de protección de datos.

Opinión sobre los alcances y aplicabilidad de la LFPDPPP y la LFTAIPF

Pregunta: Acerca de las Leyes sobre protección de datos personales (Ley Federal de Protección de Datos Personales en Posesión de Particulares y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en su capítulo relacionado a Datos Personales), ¿Cuál es su opinión respecto de sus alcances y aplicabilidad en nuestro país?

Respuestas:

- Creo que estas leyes vienen a llenar un vacío que teníamos en materia de protección a los usuarios y pienso también que en los temas financieros se ha venido sufriendo un abuso en los últimos años, que nos ha ocasionado varios dolores de cabeza, por lo cual este tipo de legislaciones nos vienen muy bien. Sin embargo, no son las únicas que se requieren y habrá que exigirle al gobierno que se actualice y vea lo que existe en otros países en la materia, de manera que se protejan los derechos a la seguridad de todas las personas y empresas en todo tipo de transacciones electrónicas y no electrónicas.

- Lo que está definido es lo que necesitamos para empezar. Lo que falta ahora es lograr los niveles de servicio para determinar el cumplimiento, los indicadores y cómo se debe implementar. Lo que nos dice la ley es lo que debes cumplir. Lo que dirá el reglamento será lo que debes hacer. Pero hace falta el cómo implementar para cada tipo de necesidad, basado en lo que realmente se requiere. Está aún abierto lo que se define para cumplir, pero aún no se precisa si es correcto al nivel que se requiere.

- Como mencionaba, sin ser un experto en ese aspecto particular, los qués están definidos. Creo que es un primer buen esfuerzo, ahora necesitamos un grupo interdisciplinario (leyes, tecnología, auditoría, aplicaciones, seguridad integral, etc.) para definir los cómos mínimos

necesarios, lo que podría conducir a certificaciones en esta materia. En general veo estas leyes con buenos ojos, ya que estábamos rezagados nuevamente frente a otros países.

- Desde el punto de vista de su alcance, me parece correcto, porque nos pone en protección del riesgo que hay por el mal uso de algunos mafiosos, o que molestan y trasgreden nuestra intimidad.

- Yo creo que este proyecto, como todos los proyectos, depende de los recursos que tiene asignados. La conciencia que debe hacerse es que no sólo son los recursos del gobierno o de las empresas, sino también de todos y cada una de las personas que estamos involucrados.

- El IFAI y la Secretaría de Economía deben hacer una labor de educación, difusión, conciencia, insistencia en entender, a través de foros sencillos, más elaborados y complejos, con grabaciones de la explicación de los puntos más sencillos hasta los más complejos, y de cómo implementar las protecciones, a través de la conciencia, con los mismos mecanismos de control de accesos a la información automatizada, o con los mismo mecanismos de enseñanza y corrección que hoy por hoy existen, pero que se diga específicamente la materia de lo que se protege y cómo se puede proteger.

- Hacer un ejercicio con una Institución tipo simple, que permita definir los riesgos sobre la información privada, y dónde reside, con qué mecanismos de control se protegen.

- Hacer mención de las políticas, normas, estándares y procedimientos, instructivos que contienen, para que sirvan de guía a quienes se encargan de diseñar, implementar, operar, vigilar y supervisar cada uno de los controles.

- Saber cómo se pueden dar los incidentes y cómo se han ido resolviendo, no con el afán malicioso de saber cómo se trasgredió la norma, sino con el afán sano de corregir debilidades y fortalecer controles que permitan resolver el desconocimiento, la instrucción, desarrollar las habilidades y controlar el buen uso de la información.

- Que la SEP y las Universidades hagan su programa similar, motivando a cada director, académico, profesor, instructor, administrativo y vigilante, a que conozca de lo que se trata pero también aplique su normatividad, procedimientos y controles.

- Muchas empresas ya tienen habilitados los mecanismos de Control de Acceso, pero hace falta se unan al esfuerzo de concienciación e implementación de un programa interno que renueve las actitudes y los propósitos de reforzar esta protección.

- Que la Secretaría de Economía en tres niveles de madurez realice las normas y que se vayan ya liberando bajo el contexto de Borrador, de documento a revisión y a optimización y documento final a implementar.

- Lamentablemente la situación de seguridad nacional que se vive en México limita la credibilidad y el uso de ambas leyes. Desafortunadamente pocas personas están convencidas de proporcionar su información privada debido a que cualquier persona puede abusar de esos datos que no están protegidos, no sólo por medios físicos o tecnologías, sino por las mismas

leyes y aunque existiesen leyes que cubren el cien por ciento de la protección de la información, la seguridad es una cuestión de ética y cultura de los individuos, en donde actualmente en estos tiempos México vive una situación crítica en materia de seguridad en todos los niveles. El enemigo número uno a atacar es la ambición por el poder y los bienes materiales y su contraparte es la ética, la moral y las buenas costumbres, que deben ser temas constantes en todos los niveles educativos.

- Desconozco sobre estas materias, pero sí puedo asegurar que si se venden bases de datos por diversas formas, ya sea del ámbito oficial, bancario o empresarial, esto quiere decir que si existen leyes para proteger la confidencialidad de los datos, no operan o su aplicación se encuentra en el total olvido.

- La aplicación de la nueva Ley será benéfica para la sociedad mexicana porque establece con claridad las reglas para todos los involucrados: empresas, ciudadanos, gobierno y organizaciones civiles. El alcance de la Ley ubica a México en la esfera internacional, porque por primera vez se contará con los mecanismos jurídicos y administrativos para regular la privacidad de las personas.

Artículos especiales sobre la Protección de Datos Personales

Las Tecnologías de Información y la Lucha por la Privacidad

Por Juan Francisco Serrano
Director General de Joint Future Systems

El mundo se encuentra en un momento muy interesante en donde el acceso a información personal, a través de la tecnología, está alcanzando niveles que ni siquiera podían imaginarse hacia algunos años.

Las redes sociales, de por sí diseñadas para compartir información, se están integrando entre ellas y directamente con cientos de aplicaciones informáticas. Las personas que se quejan mucho de que Internet y las Redes Sociales no son muy seguras ni privadas, harían bien en recordar que nunca fueron diseñadas para tal efecto y que, lejos de ser su prioridad, son precisamente lo contrario, si bien poco a poco han integrado algunos elementos de privacidad en sus diversos sistemas.

Anteriormente, lo más difícil en informática era poder comunicar un sistema con otro. Actualmente, las redes de comunicación y la interoperabilidad entre prácticamente todos los sistemas informáticos, a nivel compartición de datos, es casi absoluta. Esto incluye a los sistemas operativos de dispositivos móviles, teléfonos inteligentes y hasta consolas de juegos y televisiones avanzadas.

Hoy en día, los individuos se encuentran asediados por una continua serie de solicitudes de datos personales, desde formatos gubernamentales, hasta contratos de servicios, pasando por ofertas comerciales. Todo el mundo está capturando datos de personas.

En algunas redes sociales podemos poner fotos de conocidos, con todo y su nombre, y publicarlos no sólo a nuestra red, sino a la de conocidos y/o amigos, y a los amigos y/o conocidos de éstos.

En este entorno, la privacidad se está convirtiendo en un tema de mucha importancia. ¿Cómo protegerla? ¿Cómo recibir sólo la información que queremos y de quien queremos?

Existen varios esfuerzos por proteger la privacidad, que van desde sistemas tecnológicos (anti-spam, por ejemplo), hasta legislación (la Ley de Protección de Datos Personales en México, por ejemplo). Sin embargo, no hay sistema ni ley que pueda controlar de manera absoluta lo que sucede con nuestra información ni quién tiene acceso a ella.

La mejor defensa es que cada persona proteja su propia información. Aquí damos algunas recomendaciones para hacer esto.

1. Hay que entender que es imposible que no haya información publicada en diversos sitios en Internet respecto de nosotros. Cada vez que llenamos un formato en línea para poder acceder

a un sitio, o nos registramos en algún sistema, cabe la posibilidad de que estos datos terminen siendo públicos.

2. Se recomienda tener varios perfiles para llenar formatos. Un perfil es el que le llamaremos Perfil Público. Creemos este perfil únicamente con la información que no nos importe sea pública. Utilicemos este perfil para acceder a sitios o para llenar formatos de empresas u organismos en los que no confiamos plenamente o que no son importantes para nosotros. Un segundo perfil es el Perfil Oficial, el cual utilizaremos únicamente para llenado de documentación oficial. Puede haber varios Perfiles Alternativos, que pueden corresponder a actividades, como por ejemplo un Perfil Profesional o un Perfil para cierto tipo de “Hobbies” o Aficiones.

3. Cuidemos la cantidad de información que publicamos en Redes Sociales. Limitémosla a la que nos sentimos cómodos compartiendo con la mayoría de la gente. Utilicemos también las herramientas de privacidad que ofrecen la mayoría de las Redes Sociales, si queremos mantener algo de esta información oculta, salvo en el caso de algunas personas a las cuales expresamente autorizaremos para verla.

4. Seamos muy claros con las personas que sí tienen acceso a nuestra información, respecto de que no tienen nuestra autorización para compartir ciertos datos con otras personas.

5. Cuando veamos un dato no autorizado por nosotros (por ejemplo una foto que otra persona ha publicado), si el sistema nos lo permite, borrémosla, y si no, pidamos a la persona que la publicó que la elimine. Inclusive hay algunos recursos legales si la persona lo hizo de mala fe, que pueden solicitarse para que la foto o documento sea quitada. Por ejemplo, tanto Twitter como Facebook responden a peticiones legales en las cuales un usuario solicita que se tome x o y acción sobre información que se encuentra en sus sitios, tanto para quitarla como para compartirla, dependiendo del caso. Estos recursos sólo aplican, evidentemente, en casos considerados como "graves" por este tipo de empresas.

6. Manejemos la menor cantidad de datos muy sensibles (como por ejemplo datos bancarios) dentro de sitios de Internet. Es mejor tener una sola tarjeta para compras en línea, lo cual nos permite identificar rápidamente si se está haciendo mal uso de ella.

7. Hagamos búsquedas en Internet de nuestros propios datos, para ver si alguien está publicando algo que no queremos, o si hay información privada que no hemos protegido bien.

8. De ser posible, incluyamos algún dato que nos permita saber si un sitio u organización en particular está divulgando nuestra información. Por ejemplo, añadir un caracter en algún campo (exclusivamente de un sitio o formato de una empresa), como el nombre o la dirección, de tal manera que, si lo encontramos en otro lugar, podamos saber cuál fue la fuente de divulgación.

Con los avances de tecnología, la privacidad ya no sólo se refiere a datos, sino inclusive a información como dónde estamos en determinado momento, cuáles son nuestros movimientos y hasta con qué personas estamos. Siempre existirán, sin embargo, medidas tecnológicas y de procedimiento que ayudarán a mantener nuestra privacidad.

Para aquéllos que se preocupan de más por este tema, pueden sentirse mejor si consideran que esta materia no es nueva ni privativa a nuestra época. Cuando se creó el Registro Civil, en cada país del mundo que lo iba implementando hubieron voces que reclamaron que esto era un atentado contra la privacidad. El impuesto sobre la renta, cuando se inventó, generó una reacción similar.

Toda tecnología o procedimiento puede ser utilizado para bien o para mal. Lo importante es asumir la responsabilidad que tenemos de cuidarnos a nosotros mismos y ayudarnos con la tecnología, la legislación y los procedimientos adecuados.

Recomendaciones prácticas para la aplicación de la LFPDPPP

(Ley Federal de Protección de Datos Personales en Posesión de Particulares)

Por Raquel Pereira, Tomás Arroyo y Manuel Ballester

RESUMEN:

La aplicación de las medidas reglamentadas previstas en el Artículo Transitorio Segundo de la Ley Federal de Protección de Datos en Posesión de Particulares y en concreto aquellos que se desarrollan en el artículo 10 de la citada LFPDPPP, no solamente es un asunto de cumplimiento de la legalidad vigente, sino que también debe considerarse, como un buen mecanismo para controlar y por tanto minimizar los riesgos que afectan al tratamiento de Datos en aspectos, sobre todo de Integridad y Confidencialidad.

El presente documento es una base sustentada en la práctica además de una referencia para uso del gestor de la empresa responsable de la base de datos, al amparo de la legislación vigente sobre Protección de Datos de Carácter Personal y otros desarrollos legales que le son factibles de ser aplicados.

Todas las medidas aquí expresadas tienen que estar dotadas de la prueba auditable correspondiente, ya que reglamentariamente estarán sujetas a la auditoría interna o externa, a la inspección o verificación del IFAI (Instituto Federal de Acceso a la Información y Protección de Datos) e incluso a los tribunales de Justicia.

INTRODUCCIÓN:

La privacidad de las personas es un concepto situado en un entorno indefinido, quizá "virtual".

Otros conceptos como, la clasificación de los clientes, patrones de conducta "comercial o personal" e incluso los gustos o preferencias de las personas, son igualmente indefinidos. Sin embargo las Tecnologías de Información (TI) y su utilización por las empresas ha conseguido determinar un cierto grado de definición, esquemas y acotamientos que le han permitido a las mismas proceder a tratar estos como datos objetivos, contables y estructurados. Todo lo anterior ha sido posible porque se han establecidos procesos específicos para ello, cualquier dato es susceptible de ser manipulado estableciendo procesos.

En este entorno actualmente, la parte de privacidad que es factible moldear más fácilmente y que permite establecer procesos es el tratamiento de información de Carácter Personal, son datos que ya se están tratando en los procesos de negocio y por tanto la Legislación solamente viene a añadir condiciones y reglas a estos tratamientos.

Los profesionales, que tengan alguna relación con el tratamiento de Datos, en general, tienen la obligación de conocer y divulgar su "oficio" y por tanto el entorno legal en el cual se desarrolla, sin embargo en el ámbito de las TI, con frecuencia existen gestores que las administran y personas que dirigen grandes centros de tratamiento de información que adolecen de un profundo desconocimiento de las leyes que les afectan.

Esa situación y la necesidad del cumplimiento de la legislación alimentan en una gran cantidad de casos, un perverso sistema de búsqueda y delegación de responsabilidad, que tiende a considerar un responsable único del cumplimiento, e incluso de la vigilancia de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) al encargado de la Seguridad Lógica en la empresa.

Esta circunstancia tiene demasiado riesgo cuando en una corporación o grupo de empresas, agrupadas a través de una MATRIZ, se realizan en los mismos equipos y por las mismas personas tratamientos de datos que corresponden legalmente a varias empresas del grupo, lo que es factible de constituir una cesión de datos entre las empresas del grupo que hay que regular internamente y para la cual hay que obtener los consentimientos requeridos por la legislación.

Cada empresa es responsable de sus propios tratamientos de los efectos legales de protección de datos, la legislación afecta por separado a todas y cada una de las empresas que conforman el grupo y tiene responsabilidad con los datos que le han sido encomendados por los titulares de los mismos.

La legislación define Dato de Carácter Personal a cualquier información concerniente a personas FISICAS identificadas o identificables, la entidad debe ocuparse de la misma forma de cualquier otro dato e información que requiera para sus actividades. De facto, el sentido común y conocimiento del entorno del legislador se hace patente en el Artículo 19 de la LFPDPPP, determinando que el nivel de protección que la empresa tenga para su información, es aplicable también a los datos de carácter personal y por tanto, de alguna manera, infiere a que se utilicen los sistemas de protección para englobar cualquier información que la empresa trate, independientemente que sean datos de carácter personal, contable, fiscal, entre otros.

En consecuencia los requerimientos mínimos de protección que se establezcan en el reglamento de la LFPDPPP deben integrarse en los sistemas de protección que la empresa posea sirviendo, por tanto para cualquier tipo de información sobre la que se efectúen tratamientos. Si bien las medidas que el Reglamento determine tendrán consideración de

mínimos, debiendo ser complementadas con otras más exigentes en virtud del análisis de los riesgos a que se esté expuesto y alineadas con la clasificación de la información que corporativamente se realice.

Además en la práctica, una vez establecida una política general y unos procedimientos es más eficiente su aplicación de forma global, sin discriminar entornos ni establecer particularizaciones que no sean estrictamente necesarias.

En la línea de lo anteriormente expresado hay que considerar que en general las empresas tienden a no clasificar adecuadamente los datos, las clasificaciones solamente se ocupan de la Disponibilidad, no tanto de la Integridad y casi nada de la Confidencialidad, desde este punto de vista, el Artículo 3 de la LFPDPPP califica a los datos sensibles de la siguiente manera: los datos personales sensibles son aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida es factible de dar origen a una discriminación o que conlleve a un riesgo grave. Considerando sensibles los siguientes datos:

- Origen racial o étnico.
- Estado de salud presente o futuro.
- Información genética.
- Creencias religiosas, filosóficas o morales.
- Afiliación sindical.
- Opiniones políticas.
- Preferencia sexual.

Esta información, en el seno interno de las corporaciones afecta de forma clara a la gestión de los Departamentos de Recursos Humanos, Servicios Médicos y Seguros, entre otros, donde es factible que existan datos no solo del propio empleado sino incluso de otros miembros de su familia. Y también se gestionan Datos con un nivel menor “nivel medio de sensibilidad” como: datos económicos y patrimoniales (nóminas, créditos, patrimonio, impuestos, pertenencias, etc.).

Todo ello independientemente de que esta información sea necesaria para la actividad principal de la empresa, como puede suceder en aquellas entidades en que este tipo de datos sean imprescindibles, en el caso de actividades ligadas a la salud, medios de comunicación, asociaciones religiosas o políticas y demás entidades cuyos sistemas de información necesiten tratar datos sensibles.

Esto genera una conclusión, la empresa tiene que organizarse al respecto, desarrollando acciones y procedimientos que afectarán a uno o varios departamentos y que cada uno de ellos realizará la parte o aspecto que le corresponda del objetivo común.

Aunque la titularidad legal de las bases de datos pertenezca a la propia empresa, o persona jurídica, en la práctica de la dinámica operativa, las acciones serán realizadas, por personas

físicas, es decir, empleados responsables de los departamentos que correspondan de las empresas, esto aporta una figura de facto que tiene que asumir las funciones de COORDINACION y que corresponde con obligaciones del RESPONSABLE DE LA BASE DE DATOS.

Al coordinador es factible definirlo como:

Persona designada por la Dirección de la empresa que asume las funciones asignadas en la LFPDPPP y actúa en nombre de la empresa, que decide sobre la finalidad, contenido, tratamiento y uso de los datos contenidos en los archivos y base de datos formando parte del negocio o entorno de aplicación y uso.

Por otra parte, y sobre todo en empresas que por su tamaño tienen una estructura amplia, las funciones del responsable de la base de datos y del tratamiento es factible recaer en departamentos diferentes, entendiendo como RESPONSABLE DEL TRATAMIENTO: Persona o departamento interno de la empresa, que se encarga de efectuar los tratamientos, automatizados o no, a petición y bajo el control del responsable (Coordinador) de la base de datos, por tanto internamente la mayoría de los casos le corresponde a el Responsable de TI.

En este sentido la LFDPPP en su artículo 30 determina que las empresas designarán a una persona o departamento con dos funciones, atender a los titulares en sus derechos y velar mediante la divulgación conocimiento y formación para fomentar la protección de datos en el seno de la organización.

Otro tema a considerar es que las medidas reglamentarias que es factible aplicar se refieren a los datos y a todas sus copias, datos de prueba reales, nuevos aplicativos, soportes físicos, (disquete, cinta, cartucho, disco duro del PC, CD, listados o fichas en papel, videos, microfilm, grabaciones de audio, etc.), la computadora y almacenes, los edificios, las líneas de comunicaciones, tanto las internas como externas, los camiones y vehículos destinados al transporte de soportes, y a todas las personas que intervienen en el proceso, desde el operador al gestor de comunicaciones, el guardia de los edificios o el encargado de retirar y destruir el papel o soportes en general. Entornos que no suelen estar bajo la responsabilidad del Departamento de Sistemas.

A continuación y en un sentido práctico se mencionan acciones que se recomiendan a la empresa, estas actividades son factibles de concretar organizativamente mediante su agrupación en una Oficina Técnica de Cumplimiento para, controlar y por tanto minimizar el riesgo de un incumplimiento legal cuya consecuencia es factible de llegar, incluso a la desaparición de la entidad.

PARTE 1 – COORDINADOR DE LA BASE DE DATOS

Con carácter general, el coordinador o administrador de la base de datos tiene que impulsar procedimientos internos de Control para uso propio y de los distintos departamentos que gestionan Datos Personales, así como conocer el contenido, uso y finalidad de la base de datos de los cuales son responsables. Las funciones del coordinador son:

1.- CALIDAD DE LOS DATOS

1.1 Revisar que los datos son adecuados y no excesivos para el logro del objetivo.

1.2 Autorizar el uso y objetivos de la base de datos y asegurar que los datos sólo son utilizados para la finalidad de su recolección.

1.3 Asegurar que los datos son exactos y veraces.

1.4 Recoger los datos mediante consentimiento, contrato o fuentes accesibles al público y nunca por medios fraudulentos, desleales o ilícitos.

2.- DERECHO DE INFORMACIÓN Y CONSENTIMIENTO EN LA RECOLECCION DE DATOS

2.1 Comprobar que se informa a los afectados de forma expresa, precisa e inequívoca, mediante los correspondientes **Avisos de Privacidad** informativos en los impresos de autorización o contratos.

2.2 Las cláusulas informativas (avisos de privacidad) son revisadas por la Asesoría Jurídica.

2.3 Comprobar que se recolecta el consentimiento inequívoco del afectado mediante su firma en los contratos o impresos de autorización.

2.4 Se archiva como prueba del consentimiento durante el tiempo que dure la relación más 6 años.

2.5 Se dispone de procedimiento para la exclusión de los afectados que revoquen el consentimiento.

2.6 En los datos personales sensibles, cesiones de datos o donde sea requerido el consentimiento expreso garantizar que se obtiene inequívocamente y se archiva la prueba.

3 SEGURIDAD DE LOS DATOS

Este apartado está contenido en el Reglamento de la LFPDPPP, se mencionan una serie de Estándares de Protección/seguridad y privacidad que son básicos:

3.1 Clasificación de la base de datos en niveles de sensibilidad con fundamento en los datos que contienen, la información y finalidad de los mismos.

3.2 En general el nivel de sensibilidad se clasifica en tres:

- 3.2.1 Nivel Alto (datos sensibles).
- 3.2.2 Nivel Medio (datos económicos y patrimoniales).
- 3.2.3 Nivel Básico (todos los que no sean Alto o Medio, es decir, datos identificativos).

3.3 Crear o encargar la documentación donde se determinen las medidas de seguridad según el nivel (**Documento de Seguridad).**

3.4 Nombrar formalmente un Responsable de Seguridad.

3.5 Divulgar y entregar a cada persona una autorización expresa, junto con las normas de protección para el tratamiento, cuando se traten datos fuera de los lugares físicos de ubicación de la base de datos (TELETRABAJO).

3.6 Definir y documentar las funciones y obligaciones del personal con acceso a los Datos Personales.

3.7 Emitir Normativa, o mediante charlas, divulgar las normas de seguridad y consecuencias en caso de incumplimiento.

3.8 Crear y gestionar un Registro de Incidencias de la base de datos.

3.9 Establecer los criterios y nombrar, formalmente, las áreas de administración de control de accesos.

3.10 Autorizar formalmente la salida de soportes que contengan datos de carácter personal.

3.11 Establecer los controles periódicos del Documento de Seguridad.

3.12 Encargar Auditorías de verificación del cumplimiento legal.

3.13 Adoptar las medidas correctivas adecuadas según los dictámenes de Auditoria en cuanto al Documento de Seguridad.

3.14 Autorizar la ejecución de procedimientos de recuperación de datos.

3.15 Requerir del Responsable de Seguridad y revisar el informe de revisiones y problemas del registro de accesos con la periodicidad que el Reglamento Determine.

4 ACCESOS Y COMUNICACIÓN DE DATOS

4.1 Revisar los contratos, junto con el soporte de una Asesoría Jurídica, que se realicen con terceros (Encargados de Tratamiento), incluyendo cláusulas de finalidad, medidas de seguridad y control, comunicación, gestión de incidencias y devolución de los datos mientras esté vigente la relación contractual.

5 DERECHOS DE LAS PERSONAS

5.1 Garantizar el derecho de Acceso, Rectificación y Cancelación. (Deben existir normativa y procedimientos al respecto).

5.2 Hacer efectivo el derecho de acceso, rectificación, cancelación y oposición, en el plazo previsto por la LFPDPPP (20+15 días).

5.3 Comunicar inmediatamente a los titulares de cualquier vulneración de seguridad significativa en cumplimiento del Artículo 20 de la LFPDPPP.

6 INVENTARIO, REGISTRO, REVISIONES y CESIONES

6.1 Realizar un inventario de la base de datos corporativa.

6.2 Realizar un inventario de las bases de datos Departamentales o Locales.

6.3 Impulsar procedimientos para :

- 6.3.1 Controlar y Corregir las Incidencias.
- 6.3.2 Controlar y Corregir Accesos.
- 6.3.3 Controlar Usos y Finalidades.
- 6.3.4 Controlar Cesiones de Datos.
- 6.3.5 Resolver las peticiones por parte del Afectado sobre sus Propios Datos, según el punto 5.

6.4 Comprobar que en los contratos o impresos de autorización están incluidas las cesiones, cuando éstas existan.

6.5 Comprobar que se eliminan los informes de incumplimientos contractuales a los 72 meses (6 años).

6.6 Comprobar que los tratamientos con fines de publicidad se realizan previo consentimiento del interesado o mediante un mecanismo Legal que lo sustituya (fuentes accesibles al público y que no se han ejercido derechos de oposición al mismo).

6.7 Impulsar la creación y recibir los “Cuadros de Mando” sobre la situación de la base de datos de su responsabilidad.

Los modelos organizativos suelen diferenciar claramente las áreas de gestión del negocio con las de apoyo al mismo, aquéllas cuyo cometido es proporcionar los medios para que éste pueda desarrollarse.

PARTE 2 – RESPONSABLE (DEL TRATAMIENTO)

Esta figura de Responsable del tratamiento, asume las labores derivadas de los procesos informáticos, sobre los datos personales, siendo a su vez el interlocutor con el Responsable de la base de datos (coordinador).

Impulsará la implantación de los procedimientos de Control Interno necesarios.

Se interrelaciona igualmente con las funciones del responsable de la base de datos que se determina en el artículo 11, se observa también esta distinción en el texto del artículo 14 de la LFPDPPP en cuanto a que el Responsable tiene la responsabilidad de incorporar las instrucciones del tratamiento a los contratos de servicios externos, con encargados de tratamiento y por tanto la Ley le responsabiliza del Control del tratamiento externo (Outsourcing). El modelo está ampliamente extendido en la actualidad, por lo que es conveniente llamar la atención sobre la problemática que se ha de considerar al respecto.

Asimismo se observa que las medidas aquí expresadas, tienen un contenido más técnico, siendo a su vez un complemento de las que figuraban en la parte 1 y que en gran medida se corresponden con el marco de Control que generalmente está implantado en las organizaciones, debiendo observarse no solamente para el Control y Protección de los Datos Personales sino para todos los Activos informacionales de la entidad, medidas que como se indicó anteriormente tienen que estar dotadas de la prueba auditable correspondiente al estar sujetas a la auditoría interna o externa, a la verificación o inspección del Instituto Federal de Acceso a la Información Pública (IFAI) e incluso a los tribunales de Justicia. Las funciones para el responsable son:

I.- CALIDAD DE LOS DATOS

i. Asegurar que los datos sólo son utilizados para el objetivo de su recolección.
ii. Los datos se cancelan cuando no son necesarios.
iii. Los datos se almacenan permitiendo el Derecho de Acceso.

II.- CONSENTIMIENTO DEL AFECTADO

i. Implantar y mantener un procedimiento para la exclusión de los afectados que revoquen el consentimiento para el tratamiento (lista Robinsón)

III.- SEGURIDAD DE LOS DATOS

i. Clasificación de los datos según los niveles que se determinen en el Reglamento (Básico, Medio o Alto).

ii. Crear o asignar el desarrollo del Documento de Seguridad según el nivel asignado y de acuerdo con lo que determine el Reglamento.

iii. Documentar e Implantar medidas técnicas y organizativas para regular y controlar el acceso a los datos a través de las redes de comunicaciones.

iv. Documentar e Implantar medidas técnicas y organizativas para regular y controlar el Régimen de trabajo fuera de los espacios físicos de ubicación de la base de datos.

v. Asegurar que las medidas Técnicas y Organizativas garantizan la integridad y Confidencialidad de los Datos.

vi. Borrar los archivos temporales en el momento en que no sean necesarios.

vii. Definir y documentar las funciones y obligaciones del personal con acceso a los Datos Personales en el ámbito de los Sistemas de Información.

viii. Emitir Normativa, o mediante charlas, divulgar las normas de seguridad y consecuencias en caso de incumplimiento.

ix. Entregar a cada persona un documento que sirva para divulgar las normas de seguridad y consecuencias en caso de incumplimiento.

x. Recibir y Revisar el Registro de Incidencias de la base de datos.

Dependiendo del reglamento de la LFPDPPP, los estándares aceptados estarán determinados por el nivel de los datos y son factibles de determinarse en medidas técnicas y de control. Se menciona a continuación un ejemplo:

PARA UN NIVEL DE PROTECCIÓN BÁSICO

Para este nivel se determinan medidas eminentemente técnicas y organizativas.

- Crear/Divulgar un procedimiento de Notificación de Incidencias de Seguridad.
- Crear un procedimiento para obtener una relación actualizada de los usuarios con acceso autorizado al Sistema de Información.
- Implantar un sistema de Identificación/Autenticación que garantice la confidencialidad e integridad.
- Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación.

PARA UN NIVEL MEDIO

En este nivel las medidas de seguridad técnicas se amplían mediante la adopción del control interno de las mismas, como:

- Designar formalmente un Responsable de Seguridad.
- Establecer los controles periódicos y su definición en el Documento de Seguridad.
- Comprobar que la autenticación es Personalizada e Inequívoca, evitando la suplantación y la cesión de usuarios.
- Recibir y Revisar las Auditorías internas o externas que indiquen el grado de cumplimiento y adaptación a la legislación y a estándares internacionalmente aceptados.
- Adoptar las medidas correctoras adecuadas según los dictámenes de Auditoria, plasmándolas en el Documento de Seguridad.
- Vigilar los entornos de pruebas, controlando en detalle que las pruebas anteriores a la implantación no se realizan con datos reales o éstos se protegen de forma “no menor” que los datos en el entorno real de producción.
- Requerir estos aspectos, también, de los Encargados de Tratamiento.

EN EL CASO DE DATOS SENSIBLES O DE NIVEL ALTO

- Cifrar los Datos personales de nivel alto en todas las copias que se realicen en soportes externos (Disquetes, Cartuchos, Cintas, CD, etc.).
- Cifrar los Datos de nivel alto durante el transporte por líneas de comunicaciones.
- Establecer un registro LOG que permita determinar quién y cuándo se ha accedido a los datos especialmente sensibles.

IV.- ACCESOS Y COMUNICACIÓN DE DATOS

i. Revisar los contratos que se realicen con terceros (Encargados de Tratamiento), incluyendo cláusulas de Finalidad**, Medidas de seguridad** y Comunicación de los datos mientras dure la relación contractual.

ii. Definir las medidas de seguridad a adoptar por el Encargado de Tratamiento, así como la Devolución o Destrucción de datos al finalizar la relación contractual.

iii. Vigilar y controlar si el Encargado a su vez subcontrata parte del mismo.

V.- DERECHOS DE LAS PERSONAS

i. Crear un procedimiento informático, con rastros auditables, para tramitar los derechos de Acceso, Cancelación, Rectificación y Oposición.

VI.- INVENTARIO, REGISTRO, REVISIONES Y CESIONES

i. Mantener un inventario de la base de datos corporativa.
ii. Mantener un inventario de bases de datos Departamentales o Locales.
iii. Revisar las declaraciones y regular las cesiones de Datos a terceros.
iv. Revisar las declaraciones y regular la transferencia internacional de Datos.
v. Mantener un censo de las comunicaciones de datos a entidades externas.
vi. Implantar, dentro de su ámbito de responsabilidad, el “Cuadro de Mando” sobre la situación de la base de datos con datos de carácter Personal.
vii. Comunicar al Responsable-Coordinador las Incidencias de procesos sobre datos personales.
viii. Comunicar al coordinador los cambios o modificaciones relevantes que son factibles de afectar tanto al Sistema de Información como a la organización del mismo.

Finalmente hay que tener en consideración que la Ley Federal incorpora un régimen sancionador que tendrá un fuerte impacto en aquellas empresas que, por cualquier causa, se vean afectadas por un incumplimiento. No obstante éste no tiene que ser el verdadero motivo para acometer la adaptación de los Sistemas de Tratamiento de la Empresa, como se ha comentado anteriormente, en la Ley se encuentran oportunidades para que la Dirección tome conciencia de sus responsabilidades para el Tratamiento de los Datos, que le permitan acometer una adaptación a Estándares como las normas ISO 27001 y 27002, 25999 y metodologías como CoBIT, que le llevarían a una aproximación al Buen Gobierno de TI (ISO 38500) y a un mejor cumplimiento de obligaciones o marcos de control a que sea factible estar sometida como SOX o Basilea, lo que hay que dejar claro es que estos estándares son Opciones que la Dirección de la Empresa puede impulsar, mientras que el cumplimiento legal no es una Opción sino una Obligación. Por ello es recomendable la incorporación a los proyectos de adaptación a Consultores con conocimientos o perfiles de tipo Legal, Técnico, Organizativo y de Control, que apoyen y ayuden a la Dirección en el sentido de integrar los diferentes entornos de control, incorporando modelos de madurez en sus procesos, lo que conllevaría a mejoras significativas en Eficacia, Eficiencia, Gestión y minimización de riesgos.

México y el manejo de datos personales: El antes y el después de la Ley Federal de Protección de Datos Personales en Posesión de Particulares

Por la M. en D.I.T. Cynthia Solís
Presidenta fundadora del capítulo mexicano de la Asociación Civil Internacional AGEIA DENSI

Si tuviera que elegir el tema de moda en el selecto grupo en el que convergen la materia jurídica y tecnológica, sería sin duda la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y desde luego la serie de mitos que la rodean. Existe una gran mayoría que de hecho ignora su existencia y el pequeño sector de la población que la conoce, poco la entiende.

Hagamos un análisis de la misma, de forma sucinta pero desde diversas aristas:

En primer lugar me parece pertinente aclarar que no es la primera Ley que toca el tema de datos personales en nuestro país, ya que el Distrito Federal y el Estado de Colima contaban ya con una Ley en la materia; sin embargo es la primera Ley Federal al respecto y además abroga todas las anteriores.

Otro dato importante es que tiene desde 2001 como iniciativa en las Cámaras y fue modificada varias veces antes de que quedara como la conocemos en su versión final.

Antes de entrar de lleno a los puntos críticos de la Ley, tenemos que aclarar un punto de suma importancia, y este es ¿A quiénes le aplica?, pues bien, más allá de cualquier suposición, la respuesta nos la da la propia Ley en su artículo segundo que a la letra dice:

> "…Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:
>
> I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
>
> II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial."

Lo anterior significa que existen muy pocas excepciones a las que no les aplique la Ley: desde un profesionista independiente como un médico o un dentista, pasando por un micro empresario hasta llegar a grandes empresas, universidades u hospitales.

Ahora bien, en algunas de mis conferencias me han planteado la cuestión de lo que sucede con sus datos en posesión de organismos gubernamentales, recordemos que en este caso la Ley aplicable cuya última reforma fue en 2006 es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que cuenta con un capítulo ex profeso para la protección de datos personales.

En cualquiera de los dos casos, nos queda claro que la finalidad entorno a la protección de datos personales es que sean correctamente almacenados y tratados y que no se permita el acceso no autorizado a los mismos.

Vayamos a otra pregunta de suma importancia ¿Cómo impacta económicamente esta Ley a la iniciativa privada? Esta respuesta es a geometría variable, es decir, la inversión en seguridad será directamente proporcional a la masa de datos que se maneje y a la calidad de los mismos, es decir, en el caso de un hospital al tratar datos sensibles, los mecanismos de almacenaje y la tecnología de seguridad para el tratamiento y conservación de los mismos deberán ser aún más sofisticados que en el caso de un comerciante que únicamente solicita el nombre y el teléfono de sus clientes que no sobrepasan un centenar.

Hoy en día con la entrada en vigor de esta Ley, muchas empresas de seguridad han comenzado a rentabilizar la ignorancia de las personas acerca del tema, alertando a sus clientes y haciendo énfasis en las sanciones previstas en la misma; si bien es cierto que es una Ley que prevé sanciones pecuniarias muy altas e incluso penas corporales, no se trata de adquirir el equipo de seguridad más caro, sino el que mejor se adapte a tus necesidades como empresa o como profesionista, he aquí la importancia de contar con una buena asesoría jurídica que posteriormente te lleve a tomar mejores decisiones al momento de invertir en tecnología que coadyuve al cumplimiento de las obligaciones que impone esta norma.

El camino por andar es largo, la Ley española en la materia está por cumplir ya doce años y colegas españoles con los que he tenido el honor de compartir mesa de debate, me han comentado que los primeros años fueron difíciles que conlleva un proceso de adaptación y familiarización con el tema, que requiere esfuerzos conjuntos, por parte del gobierno, de la iniciativa privada y de una buena educación al respecto.

El Instituto Federal de Acceso a la Información y Protección de Datos tiene en sus manos grandes retos y tareas respecto de la aplicación de esta Ley; me gustaría finalizar este breve artículo, haciendo referencia a uno de los organismos homólogos al IFAIPD que por experiencia propia considero un ejemplo a seguir, me refiero al organismo francés denominado Comisión Nacional de Informática y libertades (CNIL), quien se encarga de aplicar la Ley francesa de 1978 denominada Ley de Protección de Datos de Carácter Personal, considero que para ser prudentes y mesurados uno debe de hablar de lo que conoce y me consta que es un organismo que brinda a la población la plena confianza de que la ley es correctamente aplicada y además ayuda a los ciudadanos a concientizarse acerca de sus responsabilidades al momento de otorgar información personal.

México ha dado un gran paso adelante con esta Ley, sin embargo como todo precepto jurídico requiere de una correcta aplicación, de lo contrario estará lista para la colección de leyes mexicanas que no surten efecto, es momento de hacer nuestra tarea como eslabones de la cadena que llevará a nuestro país a ser un ejemplo en Latinoamérica en la materia, pero mucho antes de esto ¿Ha reflexionado en las últimas horas a quién ha compartido sus datos personales?

M. en D.I.T. Cynthia Solís, es cofundadora del despacho boutique especializado en tecnologías de la información y propiedad intelectual LexInformatica, presidenta fundadora del capítulo mexicano de la Asociación Civil Internacional AGEIA DENSI, docente y conferencista.

Autorregulación y sellos de confianza

Por Dr. Alfredo A. Reyes Krafft
Vicepresidente de Servicios Financieros de AMIPCI

¿Confiar o no confiar?... ¡Esa es la cuestión!

Esta disyuntiva representa el principal dilema de una persona al decidir la compra de un artículo por Internet. Los Sellos de Confianza originalmente surgieron para fomentar la confianza del consumidor en transacciones de comercio electrónico.

Al final de los años 90`s, a iniciativa del *Canadian Institute of Chartered Accountants* (CICA) y del *American Institute of Chartered Public Accountants* (AICPA)[1], nacen los "sellos de confianza", y fueron el detonante para que otras empresas del sector privado empresarial apoyaran este tipo de prácticas en diversas partes del mundo.

Los Sellos de Confianza son marcas (distintivos) principalmente electrónicas, otorgadas por alguna entidad privada, que se publican en las páginas Web e indican que el proveedor cumple con las leyes, códigos éticos y de buenas prácticas; brinda una mayor seguridad tecnológica y procedimental antes, durante y después de la transacción; además, establecen mecanismos alternativos para resolver controversias entre comprador y vendedor.

La autorregulación constituye una herramienta útil para los sectores comerciales o de servicios, porque se ajusta a necesidades cambiantes y por tanto, hace flexible su modificación, sin tener que pasar por el complejo aparato legislativo.

La autorregulación ha surgido como la reglamentación derivada de la autonomía privada de empresarios que tratan datos, o de las organizaciones en que se agrupan para adoptar códigos deontológicos de conducta. La autorregulación se ha fomentado desde la OCDE y también es una posibilidad contemplada en la Unión Europea en diversas disposiciones sobre tratamiento de datos personales, protección de la intimidad en las comunicaciones electrónicas y sobre el comercio electrónico. De igual forma, el grupo de Cooperación Económica Asia-Pacífico (APEC), en su proyecto Data Privacy Pathfinder, tiene el propósito de analizar e identificar las mejores prácticas en materia de privacidad y el rol de los sellos de confianza como impulsores del flujo de información a nivel internacional.

La iniciativa Pathfinder promueve el trabajo conjunto entre sector privado, gobiernos, organizaciones de consumidores y grupos de interés público en aspectos de privacidad y protección de datos, para desarrollar un sistema que permita al sector privado crear reglas globales para la protección de la privacidad de los datos personales, apoyándose en el uso de sellos de confianza para el consumidor (trustmarks).

[1] http://www.amipci.org.mx/en_los_medios.php?mcmvme=266

El objetivo es encontrar un balance entre liberar el intercambio de información electrónica para propiciar el desarrollo del comercio electrónico; al tiempo que da certeza a los ciudadanos, garantizándoles la protección y el buen uso de datos de carácter privado.

En México fue hasta el año 2007 cuando surgen los sellos de confianza, promovidos por algunas empresas representantes de la industria como una forma de hacer ver a los legisladores que también a la industria le interesaba contar con una legislación adecuada en materia de protección de datos personales.

Desde su concepción, se sometieron al Marco sobre privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC por sus siglas en Ingles) a través de avisos de privacidad y sus respectivos resúmenes.

El proyecto fue impulsado por la Asociación Mexicana de Internet (AMIPCI), con el apoyo del Gobierno Federal a través de la Secretaria de Economía (Fondo PROSOFT).

La AMIPCI revisa que la empresa o Institución que cuenta con un sitio Web en operación y que solicita el sello, cumpla con cuatro aspectos:

1. Cumplir con el marco legal aplicable a cada sector:

    a) El **sector privado** debe ajustarse a lo señalado por la Ley Federal de Protección al Consumidor respecto de proporcionar en el Sitio Web números telefónicos, dirección y demás información de la organización, que permitan al comprador realizar aclaraciones o reclamaciones; usar la información recabada sólo para los fines solicitados garantizando la confidencialidad de la misma y no ceder dicha información a terceros; evitar prácticas de envío de mensajes no solicitados, y eliminar las prácticas comerciales engañosas.

    b) El **sector público** debe cumplir con lo señalado en Ley Federal de Transparencia y acceso a la información Pública y los Lineamientos de Protección de Datos Personales.

2. Sujeción al Marco sobre privacidad de la APEC, a través de avisos de privacidad y sus respectivos resúmenes.

3. Observancia del Código de Ética de la AMIPCI.

4. Cumplimiento de los términos y condiciones establecidos en el contrato celebrado entre la AMIPCI y los titulares del sello.

Al cumplir con estos cuatro puntos se otorga el sello de confianza, y con ello se reconoce a las empresas o instituciones que promueven el cumplimiento de la privacidad de la información y están legítimamente establecidas. AMIPCI también ofrece como mediación un procedimiento entre las partes para resolver controversias entre los consumidores y los titulares del sello.

Actualmente existen cerca de 400 sitios Web que ya cuentan con este distintivo único en su tipo en nuestro país.

En el ámbito internacional, desde noviembre de 2007, la AMIPCI suscribió el Memorándum de Entendimiento con TradeSafe y ECNetwork de Japón, SOSA de Taiwán; el Instituto de Comercio Electrónico de Corea del Sur; CommerceNet y Case Trust de Singapur y TRUSTe de los Estados Unidos, que son los principales proveedores de servicios de sellos de confianza de la región Asia Pacífico y que conforman la Asia-Pacific Trustmark Alliance (ATA). En virtud de dicho Memorándum, la AMIPCI se integra formalmente a la ATA, mediante el Sello de Confianza AMIPCI, y participa en el "Pathfinder de Privacidad de APEC" y es compatible con los sellos de confianza de dicha organización regional.

Con la incorporación al grupo del sello de confianza Euro-Label se pretende en corto plazo constituir la World Trustmark Alliance.

Destaca también la suscripción, el 20 de noviembre de 2008, en el marco del "II Congreso E-Commerce Latam 2008", del Memorándum de Entendimiento entre la AMIPCI y la Cámara de Comercio Electrónico de Colombia, la Asociación Española de Comercio Electrónico y Marketing Relacional, la Cámara de Comercio de Santiago de Chile, la Cámara Brasileña de Comercio Electrónico y la Cámara Argentina de Comercio Electrónico. Las organizaciones firmantes se comprometieron a trabajar conjuntamente para la definición de un marco normativo para facilitar la adopción, el uso y el reconocimiento recíproco de sellos de confianza a nivel de Iberoamérica.

En el breve tiempo de su existencia, el Sello de Confianza de la AMIPCI se ha convertido en un método de autorregulación ampliamente reconocido en México para la certificación de las políticas de privacidad y existencia física, que a la luz de la nueva Ley Federal de Protección de Datos Personales en Posesión de Particulares, deberá evolucionar como un mecanismo legalmente válido para que la industria alcance estándares mundiales en sus prácticas de comercio electrónico confiable.

Pequeño Análisis a la Ley Federal de Protección de Datos Personales

Por Efraín Baldenebro Ortiz / CISSP, CISA, CGEIT, CRISC
Oficial de Seguridad de la Información de la Bolsa Mexicana de Valores

La protección de datos personales, es un tema que ha cobrado fuerza e interés en los últimos meses. Mucho de este interés es debido a la reciente expedición de la "Ley Federal de Protección de Datos Personales en Posesión de los Particulares (**LFPDP**)", publicada en el Diario Oficial de la Federación el 05 de julio de 2010[2].

Sin embargo hay que recordar que anteriormente ya existían leyes de protección para datos personales, un ejemplo es la "Ley de Protección de Datos Personales para el Distrito Federal (**LPDPDF**)", la cual fue publicada el 03 de octubre de 2008 en la Gaceta Oficial del Distrito Federal[3].

Ambas Leyes hablan sobre la protección de la información considerada como un dato personal y sensible, sin embargo la LPDPDF se encuentra enfocada hacia entidades públicas del Distrito Federal, mientras que la LFPDP se enfoca a la protección de los datos personales en posesión de los particulares y es de carácter Federal.

Me gustaría enfocarme principalmente al cumplimiento de la LFPDP, analizando aspectos generales de cumplimiento, algunas consideraciones que deben ser analizadas y consideradas, así como el planteamiento de hipótesis sobre posibles situaciones que podrían ocurrir.

Primeramente es necesario homologar los conceptos alrededor de qué es un Dato Personal, por lo que cito textualmente lo estipulado por la LFPDP:

- **Datos personales**: Cualquier información concerniente a una persona física identificada o identificable.
- **Datos personales sensibles**: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquéllos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Con base en estas definiciones, podemos apreciar que mucha de la información que proporcionamos para cualquier trámite se encuentra catalogada como "Dato Personal", siendo interesante cómo ahora será necesario que cada vez que se recaben estos Datos Personales, las entidades estarán obligadas a dar un aviso de privacidad con al menos la siguiente información:

---

[2] La **LFPDP** la puedes consultar en la siguiente liga:
http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

[3] La **LPDPDF** la puedes consultar en la siguiente liga:
http://www.poderjudicialdf.gob.mx/work/models/PJDF/PDFs/Legislacion/ley_datos.pdf

- La identidad y domicilio del responsable que los recaba;
- Las finalidades del tratamiento de datos;
- Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
- Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
- En su caso, las transferencias de datos que se efectúen, y
- El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

Lo anterior pudiera entenderse como una actividad obvia que las entidades deberían haber empezado a implementar desde hace mucho tiempo, sin embargo la realidad es que muchas entidades no cuentan con los procedimientos y controles necesarios para cumplir con este punto estipulado por la LFPDP, y debido a las grandes cantidades de información que pudieran llegarse a manejar todos los días, el implementar procedimientos manuales podría traer más problemas que beneficios.

Algunos temas interesantes en relación a la Privacidad de los Datos.

- La LFPDP en su artículo 10, menciona que uno de los factores en donde no es necesario el consentimiento para el tratamiento de datos personales, es cuando éstos figuren en fuentes de acceso público. Lo anterior nos dice que debemos tener mucho cuidado con la información que subimos en Internet, ya que información considerada como Personal será pública y podrá ser utilizada sin nuestro consentimiento.

- Algunos de los lugares en donde más se manejan Datos Personales son escuelas, hospitales e iglesias, y en todos los casos muchos de los datos ingresados son de menores de edad, por lo que hay que definir si:

    - La propiedad de los datos personales será exclusiva para mayores de edad.
    - La propiedad de los datos personales será controlada por los padres hasta que los hijos cumplan la mayoría de edad.
    - En caso de que un menor de edad, haya sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la LFPDP:

        - ¿Quién ejercerá los derechos para una posible indemnización que proceda?
        - ¿Los padres del menor de edad afectado podrán hacer uso de la indemnización o ésta se guardará hasta que el afectado cumpla la mayoría de edad?

La creación y aprobación de la LFPDP es un gran avance en materia legal para que las personas puedan hacer valer sus derechos sobre el resguardo y tratamiento de sus Datos Personales, sin embargo, como en todo proceso que apenas comienza, será necesario un gran esfuerzo por parte de todos (autoridades y personas) para que se implemente y cumpla lo establecido por la ley. El camino no será fácil, pero al final creo que valdrán la pena el esfuerzo.

Cumplimiento con la LFPDPPP con el enfoque de Sistema de Gestión

Por Mario Ureña Cuate
CISSP, CISA, CISM, CGEIT
Auditor Líder ISO 27001, BS 25999
Presidente de Secure Information Technologies

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) ya llegó, ya está aquí, después de tanto pedirla… y llegó para quedarse, sin embargo, como en muchos casos, la LFPDPPP nos indica el ¿Qué debemos cumplir?, pero no necesariamente el ¿Cómo debemos hacerlo?, por lo que resulta necesario recurrir al conocimiento y experiencia de los profesionales dedicados al tema de la protección de datos, así como a las mejores prácticas existentes en el mercado relacionadas con el tema.

Y cuando me refiero a profesionales dedicados, estoy hablando no solamente de consultores, sino de todas aquellas personas que participan en actividades de protección de datos en el sector privado, gobierno, organismos descentralizados, entidades reguladoras, universidades, cámaras, etc., incluyendo abogados, ingenieros en sistemas, especialistas en seguridad de la información y seguridad informática, ethical hackers, pentesters, ingenieros sociales, forenses digitales, psicólogos, especialistas en RH, etc.

El cumplimiento con esta ley no es para un solo día o para un periodo corto de tiempo, sino más bien es permanente, por lo que debemos asegurar que nuestra organización se encuentre gestionando en todo momento el riesgo de incumplimiento con la misma.

Algunos de los problemas que se pueden presentar en las organizaciones para la implementación de los procesos, controles y procedimientos necesarios para el cumplimiento con la ley son:

- Falta de apoyo e involucramiento de la dirección
- Asignación inadecuada de presupuesto
- Falta de entrenamiento y concientización
- Inadecuado análisis de riesgos
- Falta de seguimiento
- Herramientas no disponibles o inadecuadas
- Falta de actualización
- Insuficientes evidencias de cumplimiento
- Incumplimiento con los tiempos definidos por la ley

Estos problemas no son exclusivos del cumplimiento con la LFPDPPP, son situaciones que ocurren también en otro tipo de iniciativas y proyectos dentro de las organizaciones.

Para mejorar la forma de operar y prevenir algunos de estos problemas, las organizaciones han implementado Sistemas de Gestión en los últimos años y en 2011 el interés de las organizaciones hacia el uso de Sistemas de Gestión Integrales es evidente.

Los Sistemas de Gestión más relevantes en la actualidad son aquellos basados en estándares ISO tales como ISO 9001 (Sistema de Gestión de la Calidad), ISO 14001 (Sistema de Gestión Ambiental), ISO 27001 (Sistema de Gestión de Seguridad de la Información), ISO 20000 (Sistema de Gestión de Servicios de TI), así como en estándares británicos como el BS 25999 (Sistema de Gestión de Continuidad del Negocio) que cumplen con los requerimientos definidos en la especificación británica PAS 99.

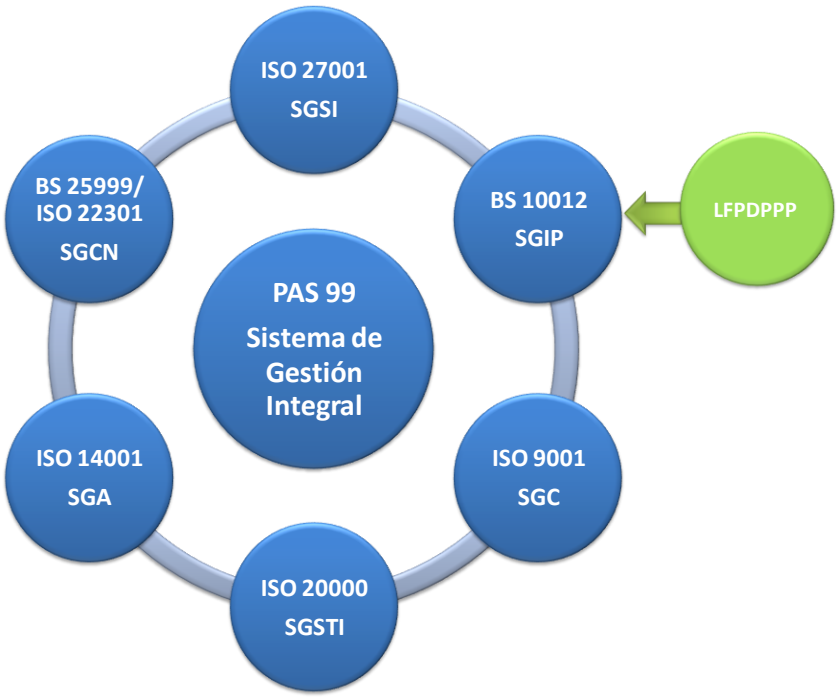


Figura 1 – Sistema de Gestión Integral

Otros estándares y mejores prácticas que utilizan el concepto de modelo de mejora continua y que complementan a los anteriores son el ISO 31000 (Gestión de Riesgos), COBIT de ISACA e ITIL de la OGC.

Resulta natural para aquellas organizaciones que ya vienen trabajando con Sistemas de Gestión, tratar el cumplimiento con la LFPDPPP a través de un Sistema de Gestión de Información Personal (SGIP), para ello es importante conocer que en la actualidad existe ya un primer estándar británico (BS 10012) que precisamente define los requerimientos que debe cumplir el SGIP.

El SGIP es la parte del Sistema de Gestión Integral que provee el marco de referencia para mantener y mejorar el cumplimiento con la legislación y buenas prácticas relativas a la protección de datos y aunque BS10012 no se encuentra 100% mapeado con la LFPDPPP, los elementos que define para las etapas de Planear – Hacer – Verificar – Actuar son totalmente aplicables.

Figura 2 – Enfoque PDCA aplicado al Sistema de Gestión de Información Personal

El detalle del proceso para la Gestión de Información Personal se define en cuatro cláusulas de éste estándar y en términos generales comprenden:

Cláusula 3 – Planear

- Establecer y gestionar el SGIP
- Alcance y objetivos del Sistema
- Política de Gestión de Información Personal
- Responsabilidades
- Provisión de recursos
- Integración del SGIP en la cultura de la organización

Cláusula 4 – Hacer

- Designación de responsabilidades
- Identificar y registrar usos de la información personal
- Identificación y documentación de información sensible
- Entrenamiento y concientización
- Evaluación de riesgos (ej. Privacy Impact Analysis)
- Mantener el SGIP actualizado
- Establecer y operar procedimientos de notificación (Incluyendo los procedimientos para ejercicio de derechos ARCO - Acceso, Rectificación, Cancelación y Oposición)
- Implementación de principios de protección de datos personales (licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad para la LFPDPPP)

- Divulgación a terceras partes
- Mantenimiento

Cláusula 5 – Verificar

- Auditoría Interna
- Revisión de la dirección

Cláusula 6 – Actuar

- Acciones preventivas
- Acciones correctivas
- Mejora continua

Algunos factores críticos de éxito para lograr el adecuado cumplimiento con la ley incluyen:

- Entender e interpretar adecuadamente los requerimientos de la LFPDPPP
- Involucramiento de la dirección
- Asegurar competencia (interna / externa)
- Planear adecuadamente antes de actuar
- Asignar el presupuesto adecuado
- Enfatizar la integración de dentro de la cultura organizacional a través del entrenamiento y concientización
- Cumplir con los tiempos requeridos por la ley.

Por supuesto que es posible cumplir con la LFPDPPP a través de la implementación de mecanismos de control exclusivamente y las disposiciones específicas que la ley contempla, sin embargo, es importante tomar en consideración el enfoque de procesos y de mejora continua para asegurar un cumplimiento permanente de la ley y no sólo eso, sino realmente contar con procesos que aseguren la protección de los datos personales.

*Nota.- El estándar para el SGIP utiliza el término “información personal” en lugar del término “dato personal”.

Mario es reconocido profesional en Gestión de Riesgos, Seguridad de la Información y Continuidad del Negocio. Es miembro del programa de formadores de opinión del BSI (British Standards Institution), miembro del CISA Quality Assurance Team de ISACA internacional, así como miembro activo de ISACA, ISC2, ALAPSI, ISSA y ALAS. Conferencista recurrente en eventos especializados e instituciones de reconocido prestigio. Mario es presidente del comité para la conferencia latinoamericana de Seguridad de la Información y Gestión del Riesgo de ISACA.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), un enfoque a la protección de bases de datos

Por Dr. Ing. Oriana Yuridia Weber
Sentrigo Inc.

La seguridad de bases de datos se ha convertido en un tema relevante en los últimos tiempos. Las bases de datos han llegado a ser un elemento de intercambio comercial y pieza clave para la obtención de grandes sumas de dinero de forma clandestina. Por ello su valor comercial se incrementa proporcionalmente a su contenido de datos financieros o a la cantidad de datos privados que contenga, el cual ponen a la venta del mejor postor. Esta economía de la información ha ido emergiendo en los últimos años y mueve miles de millones de dólares por año. Se dice que la información es poder, sin embargo para los ciberdelincuentes el poseer una base de datos con información privilegiada les otorga no sólo poder, sino también un beneficio económico oneroso.

Lamentablemente México ya ha sido víctima de la ciberdelincuencia. En abril del 2010 salió a la luz en los medios de comunicación el descubrimiento de la venta clandestina de bases de datos con información de millones de mexicanos. Estos datos personales fueron obtenidos a través de trámites diversos, como la obtención de la credencial de elector, el registro vehicular y las licencias de conducir, entre otros.

En este documento se hace un análisis objetivo de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), en adelante referida como la Ley, donde se hacen varias propuestas para la integración de conceptos concernientes a la protección de los datos electrónicos, una rama de la seguridad de las Tecnologías de la Información.

En su última versión publicada (DOF: 05/07/2010), la LFPDPPP cubre temas fundamentales en la protección de datos personales y en la definición y explicación detallada de los derechos y obligaciones del Titular, Responsable y los terceros. Además de estos temas, que sin duda alguna son muy importantes, la Ley debiera ofrecer más detalles sobre la protección mínima que el Responsable debe ofrecer para garantizar la integridad y confidencialidad de las bases de datos.

En el capítulo VI De las Autoridades, Sección I, del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), Artículo 39 de las atribuciones del Instituto, se hace referencia a diversas atribuciones de este organismo, como por ejemplo "…proporcionar apoyo técnico a los responsables que lo soliciten…" o "Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información… ".

Concerniente a este tema de protección de la información, en el caso específico de las bases de datos que es donde la información se encuentran almacenada electrónicamente, se sugiere la creación de un estándar nacional emitido por el IFAI titulado: "Normas básicas de protección de bases de datos", donde se haga referencia a temas centrales comunes en las bases de datos sin importar el tipo, la versión o el fabricante de las mismas. Los temas sugeridos a incluir son:

- Administración de la protección de datos
- Proceso de protección de datos
- Riesgos de seguridad de bases de datos
- Medidas de prevención de riesgos
- Plan de contingencia en caso de incidentes
- Planificación y diseño
- Migración de la información de bases de datos
- Operación de las bases de datos
- Auditoría de bases de datos
- Monitoreo de la actividad de bases de datos
- Normatividad internacional de protección de la información
- Certificación de :
    - Productos de seguridad de bases de datos
    - Auditores de seguridad de bases de datos
    - Empresas y/o organizaciones que ofrecen capacitación en seguridad de bases de datos
    - Empresas y/o organizaciones que ofrecen bases de datos seguras

Hasta la fecha (1ro. Noviembre 2010) no existe, en ningún país en el mundo, una normatividad que contemple todos los temas sugeridos. El crear una norma que incluya estos temas posicionaría a México a la vanguardia en legislación de protección de datos electrónicos e impulsaría la creación de nuevos perfiles técnicos en materia de tecnologías de la información.

Protección de datos y el sistema de gestión

Por: Máster Fernando Solares Valdes y Mtro. Pedro Solares Soto

Introducción

A lo largo de la historia, la humanidad se ha preocupado por ir construyendo principios y cadenas de valores para garantizar el derecho al honor y la intimidad de las personas, por lo tanto las legislaciones en materia de protección de datos nacen de la necesidad de **garantizar y proteger** información en lo que concierne al tratamiento de datos de carácter personal, por lo que este tipo de legislaciones establecen el marco para generar: **RESPALDO** para los ciudadanos contra la posible utilización indebida de sus datos personales, **RESPETO** para el tratamiento de los datos personales y otorgan un **CONTROL** al titular sobre sus propios datos.

Algunas definiciones significativas que existen en materia de legislación de datos para entrar en contexto, son las siguientes:

Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida sea factible de dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquéllos que son factibles de revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual.

Encargado: La persona física o jurídica que sola o conjuntamente con otras, trate datos personales por cuenta del responsable.

Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Titular: La persona física a quien corresponden los datos personales.

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

La legislación en materia de protección de datos en nuestro país, es un tema que tiene impacto a partir de la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010.

El alcance de la Ley de protección de datos se delimita a la finalidad de regular el tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares expresamente menciona lo siguiente: son sujetos regulados por esta Ley, los particulares: sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de: las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial. En la siguiente figura se presenta las entidades privadas donde la Ley tiene impacto.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

y su Aplicación en el Ámbito de las Organizaciones Privadas

Al cuestionar el ¿por qué cumplir con la Ley?, se tiene que tener en consideración 3 puntos de vista; el legal, el práctico y el del empresario; si se observa desde una perspectiva legal, la respuesta seria: por la necesidad de garantizar un Derecho Fundamental a la Protección de Datos, desde un punto de vista práctico, porque se establece un régimen sancionador, que va de los 100 a 320,000 días de salario mínimo y desde el punto de vista del empresario, es una oportunidad para realizar una auditoría y establecer un control del sistema organizativo y técnico.

Principios de los Datos

La importancia de los datos está en su capacidad de asociarse dentro de un contexto. Algunos principios generales de los datos se mencionan en la siguiente tabla.

PRINCIPIO	DESCRIPCIÓN
Seguridad	Adopción de medidas de seguridad dispuestas en el Reglamento de Medidas de Seguridad
Comunicación de Datos	Las cesiones que han de ser amparadas por La Ley o ser consentidas por el titular de los datos
Acceso por cuenta de Terceros	Empresas y entidades que prestan servicios, como por ejemplo las gestorías y empresas informáticas
Consentimiento	Exige una manifestación de la voluntad libre e inequívoca del titular de los datos
Transparencia (información en la recolección de datos)	Se ha de cumplir con el deber de informar de lo expresamente dispuesto en la LFPDPPP

Otros principios son: de licitud, calidad, proporcionalidad y lealtad. La licitud se refiere a que los datos sólo podrán ser tratados de forma leal y lícita. No es factible recolectar los datos de manera desleal, ilícita o fraudulenta. Los datos que se recolecten sólo serán tratados de acuerdo a finalidades determinadas, explícitas y legítimas del responsable de la base de datos, esto significa que es necesario informar y dar a conocer cuáles son estas finalidades. No es factible que sean utilizados para otras finalidades sin el consentimiento del afectado. Si son utilizados en la publicidad u otras cuestiones, hay que informar de los usos y finalidades para solicitar la autorización correspondiente. Sólo se recolectan los datos necesarios, no hay que excederse, por ejemplo cuando en un cuestionario se soliciten datos hay que determinar cuáles son los necesarios para conseguir la finalidad.

El principio de calidad se refiere a que los datos se actualizarán cuando se conozca una nueva situación del afectado. La actualización de los datos es un gran problema en la mayoría de las empresas, no es factible asegurar que los datos que manejan estén actualizados debido al esfuerzo que supone el realizarlo.

Los datos se cancelarán cuando hayan dejado de ser necesarios. Se tiene que establecer un periodo de caducidad, el problema es saber cuándo han dejado de ser necesarios y conocer que legislación afecta para tener en cuenta los periodos que imponen, así como determinar una limitación en el caso de los datos especialmente sensibles, que será el mínimo para cumplir la finalidad.

El principio de información se presenta cuando se vayan a solicitar datos personales; es necesario informar de lo siguiente:

- La identidad y domicilio del responsable que los recaba.
- Las finalidades del tratamiento de datos.
- Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.

- Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley.
- En su caso, las transferencias de datos que se efectúen.
- El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

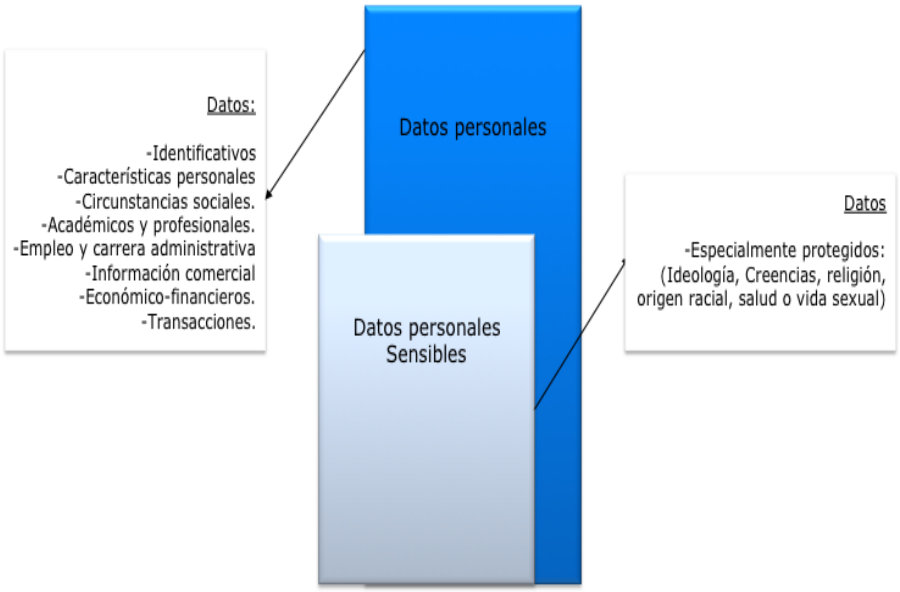
El principio de consentimiento: para realizar un tratamiento de datos se exigirá el consentimiento inequívoco, a no ser que la Ley diga otra cosa. El consentimiento se tiene que solicitar de dos formas: primera, para un tratamiento o serie de tratamientos concretos, y para unas finalidades determinadas y legítimas. Segunda, en caso de cesión de los datos, se debe de informar a quien se van a ceder los datos y sus finalidades, para que el afectado tenga la opción de oponerse a estas cesiones.

El consentimiento se tipifica en expreso o tácito. Es expreso cuando así lo solicite la Ley (datos especialmente protegidos, cesiones, otras finalidades envío de publicidad), es tácito en el resto de los casos. Siempre existe la posibilidad de retirar el consentimiento. No será necesario el consentimiento para el tratamiento de los datos personales cuando:

- Esté previsto en una Ley;
- Los datos figuren en fuentes de acceso público;
- Los datos personales se sometan a un procedimiento previo de disociación;
- Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- Exista una situación de emergencia que potencialmente sea factible en dañar a un individuo en su persona o en sus bienes;
- Sean indispensables para la atención médica.

Niveles de Seguridad

Los datos se clasifican en niveles de seguridad según la interferencia en la INTIMIDAD del individuo, estos datos se clasifican en; datos personales y datos personales sensibles. Ejemplos de los primeros son: datos identificativos como, características personales, circunstancias sociales, académicos y profesionales, empleo y carrera administrativa, información comercial, económico-financieros y los relacionados con transacciones. Los segundos se encuentran directamente ligados a datos especialmente protegidos como: ideología, creencias, religión, origen racial, salud o vida sexual. La siguiente imagen ilustra los 2 niveles de seguridad:



Tipificación de los Niveles de Seguridad de los Datos

Derechos de los Titulares

Se han de respetar unos procedimientos y plazos para dar respuesta a estos derechos; estos derechos son conocidos como los derechos ARCO (Acceso, Rectificación, Cancelación, Oposición). Otros puntos de la protección de datos a tener en cuenta son: clasificación de los datos conforme a su nivel de protección, cesión de datos a terceros, tratamiento de los datos por terceros, transferencias internacionales de datos, atención al ejercicio de los derechos, protección de los datos, medidas de seguridad a aplicar, tratamientos específicos de publicidad, creación de bases de datos de exclusión de publicidad, entre otros.

Sistema de Gestión y Privacidad

El objetivo de la PRIVACIDAD es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente su honor e intimidad personal y familiar.

Las organizaciones se suelen debatir entre sólo cumplir con la PRIVACIDAD o implantar las medidas necesarias para no tener incidentes. La legislación establece unas medidas de seguridad concretas, pero deja claro que la organización tiene que hacer lo necesario para proteger los datos personales. Para una organización lo que verdaderamente es importante es no tener incidentes que le sean factibles de desembocar en denuncias. Para ello se suele llegar a puntos muertos en el desarrollo de las medidas en los que el discurso es: “ya sé que es factible tener un incidente, pero es que la Ley no lo exige”. Por lo que este cuestionamiento lleva a identificar que un control para mitigar este cuestionamiento es integrar un sistema de gestión para complementar lo establecido con la Ley.

El ISO Guide 72 establece los principios básicos de un sistema de gestión donde se establece la política y objetivos de una organización y lograrlos, mediante:

- Una estructura organizativa donde las funciones, responsabilidades, autoridad, etc. de las personas están definidas.
- Procesos y recursos necesarios para lograr los objetivos.
- Metodología de medida y de evaluación para valorar los resultados frente a los objetivos, incluyendo la realimentación de resultados para planificar las mejoras del sistema.
- Un proceso de revisión para asegurar que los problemas se detectan y se corrigen, y las oportunidades de mejora se implementan cuando están justificadas.

La implantación de un Sistema de Gestión, o incluso su certificación, NO constituyen ninguna garantía de cumplimiento en lo referente a la PRIVACIDAD. El Sistema de Gestión tiene en su estructura los controles necesarios para evitar incidentes en la medida de lo posible, además de detectarlos rápidamente si se producen y darles una respuesta rápida, eficaz y ordenada así como adoptar las medidas pertinentes para que no se vuelva a repetir con un enfoque en cumplir la legislación. Si además de tener la conceptualización de cumplir con la Ley, se piensa en que los datos personales obtengan un nivel de seguridad que permita ser optimista.

¿Los objetivos de la ISO 27000 ayudan a la protección de datos personales?, esto es un paradigma que las organizaciones enfrentan, a continuación se mencionan los objetivos relevantes, que ayudan a identificar si esta norma ayuda a la protección de datos personales:

4.1	¿Ha desarrollado un análisis de riesgos de los sistemas de información?
4.2	¿Cuenta con un plan de gestión de riesgos?

5.1	¿Tiene una de política de seguridad soportada por la dirección?

6.1	¿Cuenta con una estructura organizativa (comité de seguridad o similar) que trate las cuestiones relacionadas con la seguridad?
6.2	¿Se ha valorado e incluido en el contrato a qué y porqué tiene acceso el personal externo (limpieza, seguridad física, mantenimiento del edificio, etc.)?

7.1	¿Se ha asignado a alguien la responsabilidad de cada de activo del sistema?
7.2	¿ Existe un esquema para clasificar la información?

8.1	¿Se han previsto controles y comprobaciones de seguridad con respecto a los candidatos a un puesto de trabajo, antes de que sean contratados?
8.2	¿Conocen los empleados sus responsabilidades con respecto a la seguridad y se les ha formado al respecto?
8.3	¿ Se han previsto controles y comprobaciones de seguridad con respecto a los empleados para cuando finaliza su contrato?

9.1	¿Existe un perímetro físico de seguridad para proteger las áreas donde están los sistemas y la información, al que sólo tenga acceso el personal autorizado?
9.2	¿Están los equipos protegidos físicamente para reducir las opciones de acceso no autorizado y protegerlos contra incidentes?

10.1	¿Están documentados y actualizados los procedimientos de operación y gestión de los sistemas de la información?
10.2	¿Se revisan y controla el cumplimiento de los acuerdos de nivel de servicio?
10.3	¿Se controla la necesidad de aumentar las capacidades de los sistemas estableciendo los criterios de aceptación para las ampliaciones?
10.4	¿Existen procedimientos implantados para proteger a la empresa contra software malicioso (virus, troyanos, gusanos, etc.)?
10.5	¿Se hacen copias de seguridad y se verifica que son válidas?
10.6	¿Se han implantado controles para mantener la seguridad en la red?
10.7	¿Hay procedimientos para gestionar (generar, almacenar, destruir, etc.) soportes removibles como discos, CDs, informes impresos,...?
10.8	¿Se controlan los intercambios de información con terceros mediante un acuerdo?
10.9	¿Se han previsto controles para garantizar la integridad y disponibilidad de los servicios de comercio electrónico?
10.10	¿Se monitoriza el uso de los sistemas para detectar actividades no autorizadas?

11.1	¿Están documentadas las reglas y los derechos de acceso de los usuarios?
11.2	¿Dispone de procedimientos para controlar la asignación de derechos de acceso de los usuarios a los sistemas y servicios?
11.3	¿Conocen los usuarios sus responsabilidades con respecto al control de acceso, con especial cuidado en los que se refiere a la selección y uso de passwords?
11.4	¿Cuenta con controles que garanticen que los usuarios sólo acceden a los servicios de red para los que tienen autorización?
11.5	¿Se identifica y verifica la identidad de los usuarios autorizados a nivel de sistema operativo?
11.6	¿Cuentan las aplicaciones específicas de la organización con sistemas de control de accesos?
11.7	¿Existe una política y controles para protegerse del riesgo de trabajar con portátiles o el tele trabajo?

12.1	¿Se especifican los requerimientos de seguridad necesarios para nuevos sistemas o mejoras de los actuales?
12.2	¿Incorporan las aplicaciones controles que validen los datos de entrada, el tratamiento y los datos de salida?
12.3	¿Se utilizan técnicas de cifrado para garantizar la integridad y confidencialidad de la información que requiera niveles especiales de seguridad?
12.4	¿Se aplica algún control para la gestión de los archivos relacionados con las aplicaciones propias de la compañía (software en operación, datos de prueba, fuentes, etc.)?
12.5	¿Existen procedimientos para el control de cambios en las aplicaciones de la compañía?
12.6	¿Existen procedimientos para la gestión de las vulnerabilidades técnicas de equipos, sistemas operativos y aplicaciones?

13.1	¿Se han previsto los canales adecuados para reportar los incidentes de seguridad?
13.2	¿Están asignadas las responsabilidades para la gestión de los incidentes?

14.1	¿Existe un plan de continuidad de negocio para reaccionar a la interrupción de actividades y proteger los procesos críticos frente a fallos o desastres?

15.1	¿Se cumplen, para los sistemas de información, con todos los requisitos legales, contractuales, reguladores y estatutarios (PRIVACIDAD, LPI, LSSI, Convenios, SLAs, NDAs, etc.)?
15.2	¿Verifica la dirección que se siguen correctamente los procedimientos de seguridad?
15.3	¿Están planificadas las auditorías de sistemas para reducir el riesgo de interrupciones en el proceso de negocio?

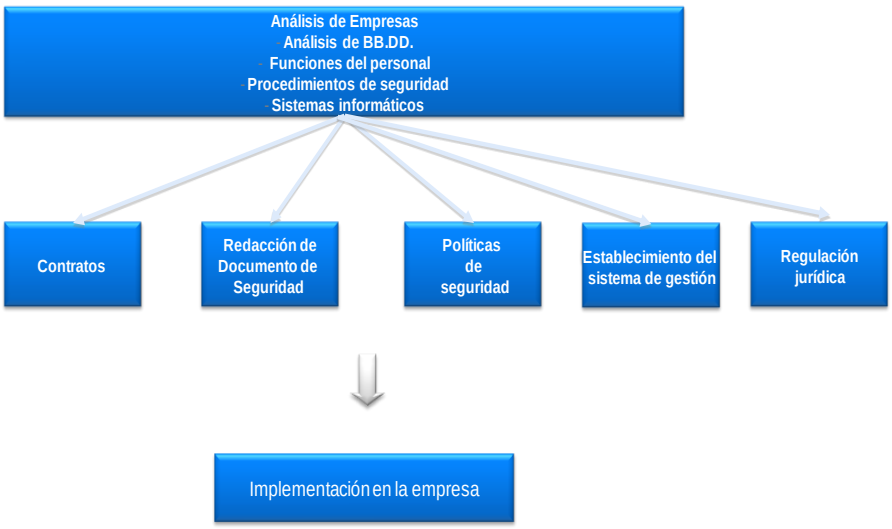
Al tener en cuenta los cuestionamientos anteriores, es factible apreciar que un gran porcentaje de los controles de la norma ISO 27000, establecen el marco de referencia más adecuado para solventar los requerimientos en cuanto a niveles de seguridad de la información en materia de la legislación de protección de datos.

Pasos para adecuar a una empresa a la LFPDPPP

Los siguiente puntos establecen algunos pasos para la identificación e inicio de la adecuación a la LFPDPPP:

- Asegurar que es factible tratar los datos y asignarles una finalidad concreta.
- Recolectar los datos de forma adecuada y poner especial cuidado en el consentimiento.
- Informar a los titulares de la identidad del responsable, de sus derechos, etc.
- Poner especial cuidado en las cesiones de datos y en realizar contratos con los encargados de tratamiento.
- Redactar un documento de seguridad. Implantación de medidas de seguridad (técnicas y organizativas).
- Respetar al máximo los derechos y principios que la Ley otorga al titular de los datos de carácter personal.
- Auditar con periodicidad temporal.

Las fases de adecuación para la protección de datos en una empresa se presenta en la siguiente figura:



Fases de Adecuación para la Protección de Datos en una Empresa

Conclusiones

Un Sistema de Gestión no garantiza que la organización cumpla con la PRIVACIDAD.

Sin embargo la mayoría de los objetivos de la ISO 27000 son de aplicación para la protección de datos personales.

La seguridad de datos personales requiere de un proceso de gestión, el establecido en la ISO 27000 está basado en el modelo PDCA que es el más difundido.

El Sistema de Gestión no garantiza que se cumpla con la PRIVACIDAD pero ayuda, y de una forma significativa.

Por ultimo si se desea cuestionar el ¿por qué adecuarse a la LFPDPPP?, las razones serian:

Sanciones.

Legislación.

Gestión segura de la información.

Crear buena imagen, prestigio.

Protección ante empleados por la incorrecta utilización de la información, del correo electrónico, Internet, etc...

Evitar principales fuentes de problemas:

Clientes insatisfechos.

Personal interno.

Competencia.

ESTUDIO DE PERCEPCIÓN
Seguridad de la Información México, 2012

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

En estos primeros meses, se está efectuando el diseño, planteamiento metodológico y definición de patrocinios, para el desarrollo de la investigación para la edición de 2012.

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

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

www.jfs.com.mx

JFS

JOINT FUTURE SYSTEMS

Av. México 19 – 701
Col. Condesa
06100 México, D.F.
Tel. (55) 5286 1839
5386 6906

E-mail: market@jfs.com.mx
www.jfs.com.mx