



Análisis de empresas de TI en materia de seguridad de datos personales para fomentar la figura de encargado de acuerdo a la LFPDPPP

## **RESUMEN EJECUTIVO**

*Julio, 2012*

## INTRODUCCIÓN

Después de varios años de análisis por el Congreso mexicano, fue publicada la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares** (LFPDPPP) el 5 de julio de 2010 en el Diario Oficial de la Federación y posteriormente, fue emitido por el Presidente de la República su Reglamento el 21 de diciembre de 2011; lo cual representa un importante avance en la tutela de los derechos constitucionales de privacidad y autodeterminación informativa, al tiempo que propicia un marco que da certeza jurídica a los consumidores y otras economías en el uso de las Tecnologías de la Información (TI).

Para la Secretaría de Economía no ha pasado por alto el hecho de que con ese nuevo marco legal se presentan grandes retos para difundir los derechos, obligaciones y deberes que ahora deben asumir los particulares y las empresas del sector de las TI que posean datos personales de personas físicas, con la finalidad de garantizar su tratamiento legítimo, controlado e informado.

En efecto, la LFPDPPP identifica como responsables del tratamiento de datos a las personas físicas o morales de carácter privado que deciden sobre el tratamiento de datos personales, es decir, cualquier información concerniente a una persona física identificada o identificable, y establece diversos principios fundamentales, entre ellos: el principio de responsabilidad, conforme al cual el responsable velará por el cumplimiento de los principios de protección de datos personales establecidos en la Ley, debiendo adoptar las medidas necesarias para su aplicación.

Lo anterior, aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable, para lo cual deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a

conocer al titular de los datos personales, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica. De la misma manera, la LFPDPPP también define la figura de **encargado** como la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

En este contexto se debe destacar que un importante número de empresas relacionadas con las TI actúan como encargados, por lo que es importante desarrollar programas que impulsen la implementación de normas o prácticas reconocidas internacionalmente en materia de seguridad, con la idea de que se promueva la confianza en su contratación y fomente la protección de los datos personales en la práctica organizacional.

Es por ello que con base en lo establecido en el PROSOFT 2.0 y el Componente F del Proyecto de Banco Mundial (Préstamo 7571-MX), se ha encomendado a la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) el desarrollo del proyecto "**ANÁLISIS DE EMPRESAS DE TI EN MATERIA DE SEGURIDAD DE DATOS PERSONALES PARA FOMENTAR LA FIGURA DEL ENCARGADO DE ACUERDO A LA LFPDPPP**", el cual busca –precisamente– fomentar entre el sector de TI la importancia en la implementación de las medidas de seguridad para la protección de datos personales.

En ese orden de ideas, el **objetivo general** del proyecto es: "Desarrollar las habilidades y fomentar el uso de buenas prácticas en materia de seguridad de datos personales en el sector de tecnologías de información para poder brindar certeza a las empresas que las subcontraten bajo la figura de encargado prevista en la LFPDPPP", y como **objetivos particulares** tiene los siguientes:

- a) Identificar habilidades y prácticas nacionales e internacionales en materia de seguridad de datos para empresas de TI.
- b) Valorar el grado de uso de prácticas de seguridad de datos personales actual en empresas de TI en México.
- c) Emitir recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI.

Una vez concluidas las 5 fases (entregables) del Estudio, se expone ahora un **RESUMEN EJECUTIVO** que condensa los primeros hallazgos, así como las recomendaciones para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de las TI.

| Entrega                      | Contenido                        | Actividades   |
|------------------------------|----------------------------------|---|
| 1ª Entrega:<br>Primer Avance | Reporte de las actividades a y b | <ol style="list-style-type: none"> <li>a) Definir la muestra de empresas del Sector de TI (del conjunto de 2,700 unidades económicas) considerando sus características específicas y el número de empresas en diferentes estados.</li> <li>b) Determinar el tipo de información a requerirse a las empresas del sector de TI para el desarrollo de la herramienta de sondeo/encuesta en línea. Se recomienda al menos la siguiente información:               <ol style="list-style-type: none"> <li>a. Actividad principal de la empresa (desarrollo de Software, servicios de TI, BPO, call center, etc...)</li> <li>b. ¿En el ámbito de sus</li> </ol> </li> </ol> |

| Entrega                                   | Contenido  | Actividades   |
|---|--|---|
|   |  | <p>actividades procesa, almacena o resguarda algún tipo de datos personales?</p> <p>c. ¿Ofrece servicios de <i>outsourcing</i> para dar tratamiento de datos personales?</p> <p>d. ¿Actualmente cuenta con medidas de seguridad?</p> <p>e. ¿Cuáles son los estándares y/o normas utilizados en la implementación de medidas de seguridad internas?</p> <p>f. ¿Cuenta con algún procedimiento establecido en caso de presentarse una vulneración de seguridad?</p> |
| <p>2ª Entrega:<br/>Segundo<br/>Avance</p> | <p>Reporte de la actividad<br/>c</p>                             | <p>c) Identificar mejores prácticas en materia de seguridad de datos personales así como los requerimientos del marco normativo previsto en la LFPDPPP.</p>   |
| <p>3ª Entrega:<br/>Tercer Avance</p>      | <p>Resultados y documentación vinculada a la actividad<br/>d</p> | <p>d) Ejecutar la encuesta a la muestra definida de empresas del sector de TI.</p>  |
| <p>4ª Entrega:<br/>Cuarto Avance</p>      | <p>Reporte sobre actividad<br/>e</p>                             | <p>e) Realizar un análisis de la información obtenida, de la cual se proyecte un esquema estadístico descriptivo sobre la</p>   |

| Entrega                      | Contenido                                | Actividades   |
|------------------------------|--|---|
|                              |  | existencia, tipo, práctica, efectividad y problemas en la implementación de las medidas de seguridad para la protección de datos personales.  |
| 5ª Entrega:<br>Quinto Avance | Reporte de actividad f y documento final | f) Elaborar recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de tecnologías de información para dar cumplimiento a la LFPDPPP. |

## **I. ÁMBITO DEL ESTUDIO (Universo de Empresas del Sector TI y Encuesta-Sondeo).**

En este apartado se resume el resultado de los entregables (avances) 1º, 3º y 4º, toda vez que están estrechamente vinculados entre sí para determinar el universo de empresas que debían ser analizadas a fin de determinar su tipo de actividad, qué tipo de datos procesan, cuáles medidas de seguridad aplican, etc., todo ello mediante una encuesta-sondeo en línea.

**I.1 Muestra de empresas del sector TI.** Con base en la metodología establecida, la primera parte del estudio comprendió actividades tendientes a definir la muestra de empresas del Sector de TI (del conjunto de 2,700 unidades económicas) considerando sus características específicas y el número de empresas en diferentes estados de la República; así como determinar el tipo de información a requerirse a las empresas del sector de TI para el desarrollo de la herramienta de sondeo-encuesta en línea.

En primer lugar se consideraron como empresas del sector de TI a todas aquellas que realizan alguna de las siguientes actividades económicas:

- a) Desarrollo de software empaquetado
- b) Desarrollo de software de sistema y herramientas para desarrollo de software aplicativo
- c) Desarrollo de software aplicativo
- d) Servicios de consultoría de software
- e) Servicios de análisis de sistemas computacionales
- f) Servicios de diseño de sistemas computacionales
- g) Servicios de programación de sistemas computacionales
- h) Servicios de procesamiento de datos
- i) Servicios de diseño, desarrollo y administración de bases de datos
- j) Servicios de implantación y pruebas de sistemas computacionales
- k) Servicios de integración de sistemas computacionales
- l) Servicios de procesamiento de datos
- m) Servicios de seguridad de sistemas computacionales y procesamiento de datos
- n) Servicios de análisis y gestión de riesgos de sistemas computacionales y procesamiento de datos
- o) Procesos de negocio basados en el uso de sistemas computacionales y comunicaciones
- p) Servicios de valor agregado de análisis, diseño, desarrollo, administración, mantenimiento, pruebas, seguridad, implantación, mantenimiento y soporte de sistemas computacionales, procesamiento de datos y procesos de negocio
- q) Servicios de capacitación, consultoría y evaluación para el mejoramiento de la capacidad humana, aseguramiento de la calidad y de procesos de las empresas del Sector de TI
- r) Servicios de administración de procesos de negocio basados en tecnologías de información que incluyen entre otros centros de

llamado, centros de contacto, administración de nóminas, carteras, cobranza, líneas de producción, entre otros.

- s) Desarrollo de software embebido (embedded software)
- t) Medios interactivos basados en tecnologías de información:
  - I. Desarrollo o creación de entretenimiento interactivo
  - II. Servicios especializados de diseño
  - III. Animación
  - IV. Tecnologías de compresión digital
  - V. Efectos visuales
  - VI. Televisión interactiva, y
- u) Cualquiera otra tecnología que el Consejo Directivo determine.

Tomando como base las actividades económicas mencionadas en las Reglas de Operación del PROSOFT 2.0 para el año 2011, se consideró un universo de 12,200 empresas para determinar la muestra que representara a dicho sector a fin de llevar a cabo una encuesta/sondeo en línea.

El diseño muestral aleatorio probabilístico consideró una muestra base de 530 empresas encuestadas a nivel nacional que, gracias a la participación interesada, permitió que ese número se incrementara a 564 empresas. El nivel de confianza de esta encuesta-sondeo en línea fue del 95%.

**I.2 Cuestionario para la Encuesta-Sondeo.** Para la encuesta-sondeo se elaboró un cuestionario integrado por 22 preguntas, que a su vez se dividieron en cinco secciones principales:

**Introducción.** En esta sección se da a conocer de manera breve el programa que el Gobierno Federal a través de la Secretaría de Economía impulsa para promover el crecimiento del sector de servicios de TI, teniendo como uno de sus objetivos particulares el fortalecimiento institucional y mejora del marco legal regulatorio y de políticas

sectoriales. Asimismo, se utilizó este apartado para dar a conocer y/o reforzar entre las empresas participantes el contenido de la LFPDPPP con relación al tratamiento de datos personales así como la figura de encargado.

**Clasificación.** En esta sección se buscó agrupar a las diferentes empresas que ofrecen servicios de TI en la industria, para las cuales la aplicación de la LFPDPPP es relevante, de acuerdo a la naturaleza de operación, misión, visión y valores. Por un lado, se realizó una estratificación del personal participante, para garantizar que la apreciación de la problemática considere las implicaciones de negocio y del ambiente tecnológico. Asimismo, se llevó a cabo la identificación del número de empleados de las empresas y el monto de sus ventas anuales. Por otro lado, se buscó detectar la existencia de empresas en el país que ofrezcan servicios de outsourcing en el tratamiento de datos personales. Una empresa con este perfil podría cubrir las características y requerimientos de la figura de encargado.

**Prácticas Organizacionales de Seguridad y Privacidad de la Información.** Con este grupo de preguntas se buscó determinar el tipo de prácticas de gestión y operación relativas a la seguridad y privacidad de la información de las empresas, que en conjunto con su naturaleza operativa, puedan ayudar a determinar las áreas de oportunidad en las mismas de cara al cumplimiento de la LFPDPPP.

**Gestión de la Seguridad y Privacidad de la Información, el cual abarcó como temas principales los procesos, roles y responsabilidades, así como la seguridad de los activos informáticos.** El objetivo principal de esta sección es determinar la forma en cómo las organizaciones han asignado las responsabilidades de seguridad de la información, así como los mecanismos de control

técnicos, operativos y de proceso encaminados a lograr el nivel de seguridad y privacidad que la operación requiere. A través de estos controles será posible identificar las medidas de seguridad administrativas, técnicas y físicas con las que las organizaciones cuentan.

**Tratamiento de Datos en el denominado Cómputo en la Nube.** En esta sección se ha buscado identificar los mecanismos de control que las organizaciones han implementado actualmente para la entrega y uso de servicios en un sistema computacional de esta naturaleza. De esta manera se podrá determinar si la industria está preparada para el cumplimiento de la LFPDPPP, manteniendo los niveles de privacidad de las personas sobre su información.

**I.3 Ejecución de la Encuesta-Sondeo en línea.** A partir de la aprobación del cuestionario, el día 9 de abril de 2012 se lanzó la invitación electrónica a las 12,200 empresas que se encontraban en la base de datos de la AMITI, la CANIETI, la AMIPCI y de la empresa encuestadora.

El periodo original considerado era de cuatro semanas, es decir, del 9 de abril al 4 de mayo de 2012, sin embargo, con el fin de alcanzar la muestra que representaría a las empresas objetivo de dicha encuesta-sondeo, se amplió dicho periodo, por lo que la encuesta en línea permaneció del 9 de abril al 31 de mayo, es decir, aproximadamente ocho semanas.

La invitación electrónica fue abierta por 4,373 empresas, de las cuales participaron 1,385 y completaron el cuestionario únicamente 564.

#### I.4 Análisis de la Información Obtenida en la Encuesta-Sondeo.

Sobre las actividades económicas que forman el sector de las TI, se detectó que menos del 5% de las empresas encuestadas proporcionan algún tipo de outsourcing.

Si se considera el tamaño de la empresa se observa que alrededor del 80% de las empresas encuestadas se encuentran en la clasificación de micro y pequeña empresa.

Ahora bien, respecto al procesamiento, almacenamiento o resguardo de datos personales –ya sean internos o de clientes– se presentaron los siguientes rangos:

- Del 41% al 45% de las empresas evaluadas procesan datos personales.
- Del 30% al 31% almacenan datos personales.
- Solo el 25% resguarda este tipo de datos.

**Prácticas organizacionales de privacidad y seguridad de la información.** Es importante señalar que el 26% de las empresas evaluadas desconocen qué regulaciones y/o marcos referenciales se utilizan para implementar la seguridad de la información. Únicamente el 39% señaló a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares como mecanismo de regulación.

**Tipo, Existencia y Práctica de Medidas de seguridad.** El 27% de las empresas cuenta con una política central y estándares auxiliares de seguridad de información; el 22% considera como lo más relevante la seguridad de recursos humanos; el 15% se basa en los objetivos de control de cumplimiento; y el 11% considera la gestión de incidentes de seguridad de la información como lo más importante.

El 55% de las empresas encuestadas no cuenta con un Comité de Seguridad que vigile el cumplimiento, monitoreo y mejoramiento de las políticas establecidas.

El 36% de las empresas no ha definido ni acuerdos contractuales ni cláusulas con sus clientes o proveedores sobre la responsabilidad del procesamiento e intercambio de información y datos personales.

El 35% de las empresas no poseen indicadores formales de evaluación de la efectividad de la seguridad de la información. Ahora bien, aquellas empresas que sí cuentan con dichos mecanismos realizan reportes de incidentes, evaluaciones de controles generales de TI, reportes de soluciones de vulnerabilidades técnicas realizadas y/o categorización de eventos identificados por la infraestructura.

**Identificación y clasificación de la información.** En este rubro solo el 29% de las empresas encuestadas lleva a cabo una identificación y clasificación de la información como componente de su marco normativo de seguridad. Además, el 29% señaló que el área responsable de definir y administrar los criterios de clasificación de la información es la Dirección General; el 26% dijo que la responsable de dicha clasificación es el área de seguridad; y sólo el 8% de las empresas asigna dicha actividad al área de datos personales.

Cabe mencionar que en el 27% de los casos no existen criterios formales de clasificación.

**Concienciación, formación y capacitación del personal en materia de protección de datos personales.** El resultado arrojado en esta encuesta muestra que el 33% lleva a cabo la concienciación de su personal a través de correo electrónico, folletos, medios impresos, etc.

El 53% manifestó que la formación y capacitación se realiza por lo menos una vez al año en su organización. Sin embargo, es importante señalar

que el 35% de las empresas no recuerda cuándo recibió la última capacitación sobre seguridad y privacidad de la información.

**Medidas de seguridad físicas.** Las medidas de seguridad físicas han sido definidas por las empresas de acuerdo a los siguientes objetivos de control:

- Seguridad física y de instalaciones (25%)
- Inventario de activos de la información (17%) o gestión de activos

**Medidas de Seguridad Técnicas.** Las empresas encuestadas han definido las medidas de seguridad técnicas dentro de los siguientes objetivos de control:

- Operaciones de cómputo (22%)
- Control de acceso lógico (20%)
- Seguridad de desarrollo de aplicaciones (16%)
- Operación de telecomunicaciones (13%)

**Problemas en la implantación de las medidas de seguridad para la protección de datos personales.** Para que las empresas del sector de servicios de TI logren adoptar mecanismos de privacidad de datos personales en sus esquemas de seguridad de la información –que cumplan con la LFPDPPP, agregando valor a sus procesos de negocio— deberán atenderse las siguientes causas raíz de las brechas y carencias observadas en los resultados de la encuesta-sondeo:

- El 80% de las empresas del sector de TI se encuentran clasificadas como micro y pequeña empresa, en consecuencia, éstas no han conseguido la capacidad para implementar las medidas de seguridad para protección de datos personales. La carencia se debe principalmente a la falta de recursos económicos y humanos.

- La función de seguridad de la información ha sido concebida y asignada de forma permanente a un contexto tecnológico, que se desenvuelve a través de esfuerzos aislados o puntuales de aseguramiento, basados en herramientas específicas de seguridad. En muchos de estos casos, la premisa principal es satisfacer algún requerimiento de auditoría o evaluación, o bien, resolver problemas acotados.
- Se reconoce una falta de experiencia de la industria de servicios de TI para la asimilación de las regulaciones de privacidad sobre el esquema de seguridad de la información, así como para reconocer las responsabilidades de cada actor especificado en la LFPDPPP y su Reglamento.
- El enfoque de protección que se ha desarrollado a lo largo del tiempo se basa en la infraestructura tecnológica, y no en la sensibilidad, criticidad e importancia de la información para el negocio, y mucho menos con un enfoque de protección de datos personales.
- Se asignan presupuestos y recursos limitados para implantar las iniciativas de seguridad de la información y privacidad de datos personales. Esta carencia se debe a una competencia con otras prioridades de la organización; prioridades que se desprenden recurrentemente del presupuesto asignado a la función de TI. De ahí, pues, que no se logre desarrollar alternativas de seguridad y privacidad en función de los requerimientos organizacionales.
- Las restricciones de recursos han dado como resultado que la mayoría de las organizaciones encuestadas no ejecuten controles fundamentales en la esfera de seguridad, por ejemplo, análisis de riesgos

y estrategia de seguridad, estrategia de capacitación y concientización en seguridad y privacidad, gestión de incidentes de seguridad o mejora continua de la seguridad de la información.

- La remediación de estas causas raíz no se encuentra en una solución única o finita, sino en un proceso permanente de la organización por incorporar los aspectos de seguridad, privacidad y cumplimiento de la LFPDPPP y su Reglamento como parte de una cultura organizacional.

**Tratamiento de Datos Personales en el denominado Cómputo en la Nube.** La encuesta-sondeo detectó que el 53% de las empresas ofrecen o utilizan servicios de cómputo en la nube.

Se revisaron los aspectos que el Reglamento estipula en relación a las empresas que ofrecen servicios de cómputo en la nube. Y se descubrió lo siguiente: la mayoría de los proveedores desconocen o no cubren los aspectos y mecanismos que dicho Reglamento determina para garantizar la debida protección de los datos personales.

**Conclusiones Generales Derivadas de la Encuesta-Sondeo.** Con base en las respuestas de las empresas encuestadas sobre el tema de seguridad de información y datos personales, es posible plantear las siguientes conclusiones:

- El porcentaje de participación de empresas micro y pequeña, puede indicar que existe una preocupación genuina por los alcances y requerimientos de seguridad y privacidad para la industria por los esfuerzos a desarrollar en su cumplimiento.
- En el caso de la participación de empresas micro por su nivel de ingreso, es importante no restringir el presupuesto para la implantación de mecanismos de control que ayuden a cumplir con las disposiciones de la Ley. El compromiso de privacidad y seguridad de la información de los datos personales no atiende al

tamaño del negocio, sino al tipo y sensibilidad de dichos datos que se manejan en sus procesos.

- Se identifican a los servicios de outsourcing de tratamiento de datos personales como un área de oportunidad de negocios para las empresas del sector de TI en México, ya que actualmente solo el 31% lo ofrece.
- Si bien en las empresas existe cierto entendimiento sobre algunos componentes clave para el cumplimiento de la LFPDPPP, estos aún no se están ejecutando.
- Existe una percepción en las empresas evaluadas de que el tema de seguridad de datos personales debe ser resuelto por una función de tecnología de la información (TI).
- Las organizaciones han trabajado en la implementación de controles técnicos preventivos y de detección de brechas de seguridad, pero no en un contexto de privacidad de datos personales.
- La implementación de los controles actuales está basada en gran parte en la experiencia de los responsables de la función de TI.
- La mayoría del presupuesto para esfuerzos de iniciativas de seguridad y privacidad están derivados de los presupuestos de TI.
- La efectividad de las funciones de seguridad y privacidad no están siendo monitoreadas, evaluadas y supervisadas en ningún sentido.
- A partir de algunas de las opiniones de los participantes que respondieron la encuesta-sondeo, es posible identificar que las empresas consideran que este tipo de regulaciones aplica únicamente para empresas grandes.
- Actualmente las empresas no cuentan con un equipo de respuesta de incidentes ni con una bitácora de control de actividades de la infraestructura de procesamiento, aplicaciones, información y datos personales, que permitan tener un control formalizado de estas actividades. Por lo tanto, sería complicado proporcionar evidencia

en un proceso legal relativo a brechas de seguridad y afectación de datos personales.

- Considerando la naturaleza de sus servicios y su inercia operativa, el sector de cómputo en la nube debe realizar esfuerzos en la revisión de sus contratos de adhesión, en las características de entrega de servicios y en su esquema operativo, de tal forma que se adapten a los requerimientos que el Reglamento de la LFPDPPP establece en el artículo 52.
- Es importante señalar que las empresas que no reconocen la utilidad del Análisis de Riesgos, basan sus políticas de seguridad de la información en esfuerzos puntuales de remediación de desviaciones o decisiones subjetivas de los responsables de estas funciones.
- El Artículo 20 de la LFPDPPP y los Artículos 63 al 66 de su propio Reglamento, reconocen como prioritario la gestión de incidentes de seguridad de la información. En consecuencia, otra área de oportunidad de cara al cumplimiento de la LFPDPPP, se encuentra en el bajo porcentaje de organizaciones que han trabajado en la gestión de incidentes de seguridad de la información.
- La capacitación sobre seguridad y privacidad de la información representa uno de los esfuerzos más relevantes que la industria de servicios de TI debe ejecutar. Por ello, el carácter organizacional de la privacidad de datos personales en el Reglamento de la Ley implica capacitación activa para el personal de la organización que trate datos personales.

## II. IDENTIFICACIÓN DE MEJORES PRÁCTICAS

El segundo reporte de este Estudio, tuvo por objeto "Identificar mejores prácticas en materia de seguridad de datos personales así como los requerimientos del marco normativo previsto en la LFPDPPP".

Las mejores prácticas y estándares que se analizaron fueron los siguientes:

#### CMMI (Capability Maturity Model Integration)

- Conjunto de mejores prácticas que proporciona los elementos para tener procesos efectivos que ayudan a mejorar la eficiencia, eficacia y calidad dentro de los grupos de trabajo, proyectos y divisiones. En otras palabras, contribuye al mejoramiento de todas las áreas de una organización.
- La seguridad de la información puede ser concebida, dentro del modelo CMMI de desarrollo y de servicios, como un tipo de requerimiento. Sin embargo, el SSE-CMM (System Security Engineering Capability Maturity Model) lo establece de forma específica en sus 11 áreas de procesos de ingeniería de seguridad.

#### CobIT (Control Objectives for Information and Related Technology)

- Conjunto de prácticas para mejorar el manejo de la información tanto en el área financiera como en la tecnológica. Es un marco de referencia para establecer un rumbo seguro y confiable de las tecnologías de información así como una herramienta que da soporte a la alta dirección para reducir la brecha existente entre las necesidades de control, las cuestiones técnicas y los riesgos propios de un negocio.
- Dentro de los beneficios de CobIT se encuentra que los requerimientos de seguridad y privacidad serán más fácilmente identificados, y su implementación podrá ser monitoreada a través de los dominios establecidos en CobIT: Planear y Organizar (PO),

Adquirir e Implementar (AI), Entregar y Soportar (DS) y Monitorear y Evaluar (ME).

## ISO 27001

- Es el estándar internacional de gestión de seguridad de la información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad de la información a un nivel adecuado.
- En su anexo A enumera en forma de resumen los objetivos de control y controles que desarrolló la ISO 27002:2005, con la finalidad de que sean seleccionados por las organizaciones para el desarrollo de sus Sistemas de Gestión de la Seguridad de la Información (SGSI).
- En la serie ISO 27000 están en fase de desarrollo la ISO/IEC 27017 –que consistirá en una guía de seguridad para Cloud Computing— y la ISO/IEC 27032 –que consistirá en una guía relativa a la Ciberseguridad—.
- Considerando que la ISO/IEC 27001 es el estándar internacional de seguridad de la información, encontraremos en todos los dominios el criterio de aplicabilidad en la protección de datos personales. Cabe señalar que en el dominio A.15 Cumplimiento, Objetivo de Control “cumplimiento de los requisitos legales” se encuentra –de forma específica— el control 15.1.4 relativo a la protección de datos y privacidad de la información de carácter personal.
- El ISO/IEC 27001 es el estándar en seguridad de información certificable, por lo que las empresas de TI que deseen ser

consideradas como un proveedor confiable deberán tomarlo en cuenta para su estrategia de seguridad de información.

- La ISO/IEC 27005:2011 es una norma esencial para aquellos que requieran gestionar sus riesgos de manera efectiva y, en particular, para cumplir con la gestión de la información de seguridad mediante el estándar ISO/IEC 27001.

#### ITIL (Information Technology Infrastructure Library)

- Conjunto de directrices (mejores prácticas) y de módulos mediante los cuales podemos establecer un mejor aprovechamiento de los recursos informáticos de una entidad u organización, desde una perspectiva de servicios. ITIL ha trazado el camino del “cómo” obtener mayor beneficio de las tecnologías de información.
- Considerando que ITIL cubre los servicios de TI en todas sus fases, los 5 libros que lo conforman contienen procedimientos útiles, que aplican para la protección de la información.

#### NIST (National Institute of Standards and Technology)

- Su misión consiste en promover la innovación y la competencia industrial en Estados Unidos.
- Los laboratorios NIST se centran en tres áreas focalizadas: ciencia de medición, tecnología (tecnologías de la información, ingeniería) e instalaciones de usuarios nacionales.
- Las publicaciones para la seguridad informática y la tecnología de la información son los especiales de la serie 800.

- Dentro de la serie 800, los más relevantes en el tema de seguridad y de datos personales se encuentran los siguientes:

| <b>Número de Publicación<br/>(Fecha)</b> | <b>Título</b>  | <b>Contenido</b>   |
|--|--|--|
| NIST SP 800-12<br>(Octubre de 1995)      | Introducción a la Seguridad Informática: El Manual NIST  | Se enfoca a los controles de seguridad de acuerdo a su naturaleza, es decir, se hace una clasificación de los mismos (controles administrativos, operativos y técnicos).                                       |
| NIST SP 800-14<br>(Septiembre de 1996)   | Principios y Prácticas Generalmente Aceptadas para la Seguridad de los Sistemas Tecnológicos de la Información | Se describen los 8 principios y 14 prácticas de seguridad.   |
| NIST SP 800-39<br>(Marzo de 2011)        | Administración del Riesgo en la Seguridad de la Información  | Proporciona a las organizaciones una guía para la administración del riesgo de la seguridad de la información estableciendo los componentes del mismo (establecer, valorar, responder y monitorear el riesgo). |
| NIST SP 800-122<br>(Abril de 2010)       | Guía para la Protección de la Confidencialidad de la Información   | Sugiere categorizar el nivel de impacto de la confidencialidad de la PII (Información de Identificación Personal) en bajo,   |

| Número de Publicación<br>(Fecha)       | Título  | Contenido  |
|--|---|--|
|  | de Identificación Personal  | moderado y alto, y con base en el daño potencial que pudiera resultar a los titulares de la información y/o la organización si esta fuera vulnerada, utilizada o divulgada de forma inapropiada. Adicionalmente, establece que la PII debe ser protegida a través de una combinación de medidas, incluyendo salvaguardias operativas, salvaguardias específicas de privacidad y controles de seguridad.                    |
| NIST SP 800-144<br>(Diciembre de 2011) | Directrices en Seguridad y Privacidad en Cómputo en la Nube de tipo Público | Provee una perspectiva general de los servicios de cómputo en la nube de tipo público y los retos en seguridad y privacidad que conllevan. Asimismo, describe los modelos de uso (nube pública, nube privada, nube comunidad y nubes híbridas) y emite recomendaciones tanto en temas de seguridad y privacidad como de actividades a realizarse para la contratación de un servicio de outsourcing de cómputo en la nube. |

## PCI/DSS (Payment Card Industry Data Security Standard)

- Estándar internacional que establece un conjunto de requerimientos de seguridad de la información para proteger los datos de los tarjetahabientes.
- Las compañías que procesan, guardan o transmiten datos de los tarjetahabientes deben cumplir con el estándar, de no hacerlo se arriesgan a la pérdida de sus permisos para operar (pérdida de franquicias).
- La información proporcionada por los tarjetahabientes para el manejo de las tarjetas de crédito y débito es de carácter personal (datos de identificación, financieros y patrimoniales), por esta razón, cada uno de los objetivos de control y requerimientos previstos en este estándar aplican para la protección de datos personales.

## España

- La Agencia Española de Protección de Datos (AEPD) es la institución encargada de cuidar y fomentar la privacidad y la protección de datos personales en España. A su vez la Península Ibérica pertenece a la Unión Europea, por lo tanto, debe ceñirse a los criterios de ésta.
- La AEPD es un ente de Derecho público con personalidad jurídica propia y plena capacidad pública y privada conforme al Real Decreto 428/1993 del 26 de marzo de 1993.
- El artículo 9 de la Ley Orgánica 15/1999 (LOPD) del 13 de diciembre de 1999 establece que tanto el responsable como el encargado del tratamiento deberán adoptar medidas de índoles

técnica y organizativas, que garanticen la seguridad de los datos de carácter personal para evitar su alteración, pérdida, tratamiento o acceso no autorizado.

- El Reglamento de desarrollo de la LOPD establece que las medidas de seguridad exigibles a las bases de datos (ficheros) y sus tratamientos se deben clasificar en tres niveles: básico, medio y alto.
- La AEPD ha emitido un documento denominado Guía de Seguridad de Datos y la cual recoge una serie de mejores prácticas en materia de protección de datos personales.
- La clasificación de los niveles de seguridad se realiza conforme a la naturaleza de la información tratada y a la necesidad de garantizar la confidencialidad y la integridad de la información.
- Las medidas de seguridad son acumulativas.
- La Guía establece un documento de seguridad, cuyo contenido está estructurado de la siguiente forma:
  - Ámbito de aplicación del documento.
  - Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos.
  - Información y obligaciones del personal.
  - Procedimientos de notificación, gestión y respuestas ante las incidencias.
  - Procedimientos de revisión.
- El Reglamento de la LOPD establece en sus artículos 96 y 110 que a partir del nivel medio de seguridad requerido, las bases de datos

deberán someterse, al menos cada dos años, a una auditoría interna o externa, de la cual se generará un informe que se entregará al responsable de la base de datos y a disposición de la AEPD o a las autoridades de control de las entidades autónomas.

- La Asociación Española de Normalización y Certificación (AENOR) ha publicado entre otras normas relacionadas a la seguridad de la información, las siguientes:
  - Desde el 28 de noviembre de 2007: ISO/IEC 27001 como UNE-ISO/IEC 27001: 2007
  - Desde el 9 de diciembre de 2009: ISO/IEC 27002 como UNE-ISO/IEC 27002: 2009

#### Reino Unido

- El Reino Unido a través del Data Protection Act 1998 establece que –cuando se tenga un encargado para el tratamiento de datos personales— se deberá seleccionar un encargado que provea suficientes garantías sobre sus medidas de seguridad para proteger el procesamiento que hará en nombre del responsable; se debe revisar que esas medidas de seguridad están llevándose a la práctica y deberá existir un contrato por escrito donde se establezcan las obligaciones del encargado. Existe un modelo de contrato publicado por el Comité Europeo para la Estandarización.
- La Oficina del Comisionado de Información (ICO) es una autoridad independiente en el Reino Unido, que se creó para defender los derechos de información de interés público, y para promover la apertura de los organismos públicos y la privacidad de los datos de los individuos.

- En relación a las medidas de seguridad, el DPA ha establecido lo siguiente: “Principio 7: Se deben tomar medidas técnicas y organizacionales apropiadas en contra del procesamiento sin autorización o ilegal de los datos personales así como en contra de pérdida accidental, destrucción o daño a los datos personales
- Se sugiere diseñar un modelo organizacional de seguridad, acorde con el tipo de datos personales que se poseen y acorde también con las contingencias de vulneración a la seguridad de la información.
- La ICO ha diseñado notas y códigos de buenas prácticas, que a continuación se muestran:
  - Nota de buenas prácticas de datos personales. Seguridad de Información Personal (Data Protection Good Practice Note Security of Personal Information)
  - Nota de buenas prácticas para protección de datos personales (Lista de entrenamiento para pequeñas y medianas empresas) (Data Protection Good Practice Note)
  - Código de Práctica de compartición de Datos (Data Sharing Code of Practice)
  - Código de práctica de información personal en línea (Personal information online code of practice)
  - Cómputo en la nube (Cloud computing)
- El ISF –por sus siglas en inglés, Information Security Forum— se dedica a la investigación, aclaración y solución de temas clave sobre seguridad de la información y administración de riesgo a través del desarrollo de mejores prácticas

- El Estándar de buenas prácticas 2011 contempla la perspectiva empresarial para la seguridad de la información y se divide en cuatro categorías principales:
  - Gobernanza de la seguridad
  - Requerimientos de seguridad
  - Marco de control
  - Monitoreo y mejora de la seguridad

## Estados Unidos

- En el ámbito de la protección de datos personales en posesión de los particulares, Estados Unidos de Norteamérica cuenta con regulaciones en materia de privacidad y medidas de seguridad exigibles a los responsables y encargados de datos personales, tanto sectoriales como estatales.
- En el ámbito federal:
  - El Privacy Act de 1974 establece un código de prácticas justas que regulan la recolección, mantenimiento, uso y divulgación de la información de los individuos que se encuentra en los sistemas de registro de las agencias federales de los Estados Unidos.
  - El United States Code (USC) es la codificación por temas de las leyes generales y permanentes de los Estados Unidos de Norteamérica y se divide en amplios temas divididos en 50 títulos. Es publicado por la Oficina de Revisión Legislativa de la Cámara de Representantes de Estados Unidos.

- Dentro del título 15 “Comercio y Negocios” capítulo 94 del USC, se considera el tema de la privacidad de la información personal. Hace un análisis en torno a la divulgación de la información personal privada y al acceso fraudulento de la información financiera.
- En la sección 1173(d) del Health Insurance Portability and Accountability Act of 1996, “Estándares de seguridad para información de salud” se establece que la Secretaría de Servicios de Salud y Humanos, deberá adoptar estándares de seguridad que tomen en cuenta las capacidades técnicas de los sistemas de registro utilizados para mantener la información de salud; los costos de las medidas de seguridad; la necesidad de capacitación de las personas que tengan acceso a la información de salud; el valor de rastros de auditoría en sistemas computarizados de registro; y las necesidades y capacidades de pequeños proveedores del cuidado de la salud y proveedores rurales del cuidado de la salud.
- En el ámbito estatal:
  - El estado de Massachusetts cuenta con un reglamento denominado 201 CMR 17.00: Estándares para la Protección de Información Personal de los residentes de Commonwealth.
  - Los objetivos del instrumento mencionado son los siguientes: garantizar la seguridad y confidencialidad de la información de clientes de acuerdo a los estándares de la industria correspondiente; proteger la información contra amenazas o

riesgos previstos; y proteger contra el acceso no autorizado o uso de la información que pueda dar como resultado un daño o incomodidad a cualquier consumidor.

- Dentro de los Estatutos Revisados de Nevada (NRS) el capítulo 603A trata específicamente sobre la seguridad de la información personal. Aquí se establece, bajo el título de “Regulación de Prácticas de Negocio” en sus artículos NRS 603A.200 y NRS 603A.210, lo referente a destrucción de ciertos registros y medidas de seguridad, respectivamente.
- El artículo NRS 603A.215 estipula que aquellos responsables que acepten tarjetas de pago deberán cumplir con la versión actual del estándar PCI/DSS. En caso de que el responsable no realice esta práctica, tiene la obligación de no transferir información personal a través de una transmisión electrónica o sin voz diferente al fax, a menos que se cifre<sup>91</sup> la información con el fin de garantizar la seguridad de la transmisión electrónica.
- Cabe señalar que otros estados como California, Hawái, Illinois y Vermont, por mencionar algunos, cuentan con legislación en materia de privacidad.
- Existen varias organizaciones gubernamentales y privadas que emiten modelos, mejores prácticas y estándares sobre seguridad de la información en Estados Unidos, por ejemplo, la Universidad de Carnegie Mellon (Software Engineering Institute)- CMMI, ISACA-CobiT o NIST.

---

<sup>91</sup> Cifrado quiere decir: “La protección de los datos que se encuentren en forma electrónica u óptica, en almacenamiento o en tránsito, utilizando: una tecnología de cifrado que haya sido adoptada por un cuerpo establecido de estándares, incluido, pero no limitado a, los Estándares de Procesamiento de Información Federal publicado por el NIST, la cual procese tales datos de forma indescifrable en ausencia de las llaves criptográficas necesarias para permitir la decodificación de dichos datos.” NRS 603A.215, <http://www.leg.state.nv.us/nrs/nrs-603a.html>, revisado el 21 de febrero de 2012, 20:00 hrs.

### III. RECOMENDACIONES Y MEDIDAS CORRECTIVAS

El quinto y último Entregable comprendió como actividad principal la elaboración de "...recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de tecnologías de información para dar cumplimiento a la LFPDPPP".

**III.1 Recomendaciones.** Para facilitar la adopción de los mecanismos de control que cada organización requerirá a partir de su análisis particular, así como sus características de operación para el cumplimiento de los requerimientos de la LFPDPPP, que se propusieron dentro del apartado "Marco práctico referencial de mecanismos de control de gestión de seguridad y privacidad de la información", es importante tener en cuenta las siguientes recomendaciones complementarias:

- El esfuerzo para estimar el nivel aceptable de riesgos, y la combinación de controles de seguridad y privacidad en la organización, puede basarse en las referencias documentales de las experiencias en otros países con regulaciones similares, y que han sido incluidos como parte de esta investigación. El uso de estas referencias no implica copiar o adaptar los elementos que se han desarrollado, sino que deben favorecer la generación de alternativas adecuadas a la realidad operativa de la organización.
- Las empresas del sector de TI deben trabajar en la redefinición de sus servicios para clientes finales, considerando los mecanismos de operación y habilitación tecnológica en que se genera el servicio de TI, y los elementos legales y de calidad del servicio que se acuerdan con los proveedores y clientes. De tal suerte que el modelo de operación atienda estos requerimientos de forma natural, y la seguridad de la información y privacidad de datos se

conviertan en atributos naturales de cada servicio ofrecido. Esta recomendación implica que se cambie el enfoque de gestión actual de la infraestructura a un enfoque integral de gestión de servicios informáticos.

Asimismo, se recomienda que dentro de las áreas comerciales de las empresas se defina todo lo relacionado al encargado de acuerdo a la LFPDPPP, considerando entre otros aspectos lo siguiente:

- Objetivo
  - Actividades técnicas a cubrir
  - Beneficios
  - Requerimientos
- 
- Una forma positiva de potenciar los esfuerzos para incrementar la seguridad y privacidad de la información, se encuentra en que la organización ejecute sus iniciativas de controles, dentro de un marco referencial de industria que pueda ser evaluado de manera independiente (certificación), y se obtenga garantía razonable de la efectividad de la gestión de seguridad considerando los requerimientos de privacidad de las partes interesadas.
  - Para apoyar las actividades de monitoreo y evaluación de la efectividad de la función de seguridad dentro de los parámetros de riesgo y privacidad, es recomendable que las organizaciones puedan instaurar un mecanismo de autorregulación desde una perspectiva de cumplimiento independiente a la operación de la infraestructura y seguridad, que favorezca la supervisión y mejora continua en el corto plazo, y a su vez, permita preparar el marco de seguridad y privacidad para una revisión externa que determine el cumplimiento de la LFPDPPP en la madurez natural de la regulación.

**III.2 Medidas Correctivas.** Como recomendaciones en materia de medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en el sector de las TI para dar cumplimiento a la LFPDPPP, se resumen a continuación las más importantes:

**Prácticas organizacionales de seguridad y privacidad de la información**

| <b>Estado general</b>  | <b>Medidas correctivas</b>   |
|--|--|
| <ul style="list-style-type: none"> <li>• Las empresas del sector de TI reconocen ciertos mecanismos como el fundamento para la toma de decisiones sobre el nivel de seguridad de la información y privacidad de datos, tales como: análisis de riesgos, cumplimiento con ejercicios de auditoría, recomendaciones de proveedores, análisis técnicos de vulnerabilidades, entre otros. Sin embargo, su ejecución no se encuentra formalizada ni se reconoce como un componente organizacional con una participación multidisciplinaria.</li> <li>• En este sentido, las organizaciones han comenzado a</li> </ul> | <ul style="list-style-type: none"> <li>• El Análisis y Evaluación de Riesgos de Seguridad y Privacidad se debe establecer como un proceso formalmente definido dentro de las prácticas organizacionales para ajustar la operación del negocio y la calidad de los servicios a los clientes, a partir de identificar las prioridades de protección con un estricto sentido de negocio.</li> <li>• A partir de la identificación de las prioridades de protección y privacidad, las organizaciones deben asignar partidas presupuestales específicas para desarrollar los proyectos de seguridad y privacidad, como</li> </ul> |

| <b>Estado general</b>  | <b>Medidas correctivas</b>   |
|--|--|
| <p>implantar mecanismos de seguridad de la información a partir de regulaciones y requerimientos puntuales.</p> <ul style="list-style-type: none"> <li>• Por lo que las asignaciones de presupuesto son limitadas y solamente se realizan, en mayor medida, asignaciones para proyectos aislados específicos.</li> <li>• La ejecución de estos proyectos de controles para seguridad y privacidad son ejecutados como parte de las responsabilidades de la función de Sistemas/Informática/TI del negocio, sin incluir un enfoque y ejecución integrales.</li> <li>• Las organizaciones identifican aquellos rubros generales de control que deben considerarse para desarrollar mecanismos específicos de protección y privacidad, sin embargo, no todos han sido implantados.</li> </ul> | <p>parte de un ejercicio estratégico de planeación de presupuesto, que corresponda al nivel de participación de todas las áreas de la organización en el uso de estos controles en sus procesos.</p> <ul style="list-style-type: none"> <li>• Las organizaciones deben ampliar los roles y responsabilidades sobre seguridad y privacidad para todas las áreas y funciones de su estructura, para que se asienten y ejecuten formalmente.</li> <li>• Se debe definir un procedimiento de estrategia de seguridad y privacidad, que aproveche los resultados del análisis y evaluación de riesgos, para la toma de decisiones sobre los rubros de control que se van a desarrollar en la organización a partir de la prioridad, factibilidad y beneficio de estos controles.</li> </ul> |

| Estado general  | Medidas correctivas   |
|---|---|
| <p><b>Gestión de la seguridad y privacidad de la información</b></p> <p><b>“Procesos, roles y responsabilidades”</b></p>  |   |
| <ul style="list-style-type: none"> <li>• Se identifica la existencia de un Comité de Seguridad de la Información que vigila las actividades de aseguramiento y cumplimiento de la privacidad de datos dentro de la organización.</li> <li>• Asimismo, se ha incrementado la participación de roles estratégicos en la clasificación de la información (tipo y prioridad de protección)</li> <li>• Las organizaciones no han ejecutado esfuerzos continuos sobre la capacitación del personal en temas de seguridad y privacidad de la información.</li> <li>• De igual forma, no se han desarrollado esquemas de medición de la efectividad de la función de seguridad y privacidad, por lo que solamente se cuenta con métricas operativas o evaluaciones técnicas esporádicas.</li> </ul> | <ul style="list-style-type: none"> <li>• Las organizaciones deben establecer formalmente (como parte del esfuerzo de asignar roles y responsabilidades), un grupo multidisciplinario que tenga responsabilidades sobre la determinación del nivel de riesgo aceptable, la definición de la estrategia de seguridad, medición de la efectividad de la función de seguridad y operación directa de controles.</li> <li>• Las organizaciones deben incluir a las áreas comerciales, de operación y jurídicas en la definición de los roles y responsabilidades de seguridad y privacidad, con una asignación puntual de la determinación de acuerdos y términos legales, niveles de servicio y desviaciones relativas a brechas de seguridad e incidentes para con proveedores, socios de negocio</li> </ul> |

| Estado general   | Medidas correctivas  |
|--|--|
| <ul style="list-style-type: none"> <li>Las implicaciones de los requerimientos de privacidad, no se han considerado en los acuerdos contractuales con proveedores, socios de negocio ni clientes.</li> </ul> | <p>y clientes.</p> <ul style="list-style-type: none"> <li>En el primer esfuerzo de mecanismos de control, las organizaciones deben definir y ejecutar una estrategia integral de concientización sobre seguridad y privacidad de la información, dentro de los parámetros corporativos de comunicación institucional.</li> <li>Como parte de los controles relativos a la gestión de incidentes y brechas, deben derivarse componentes de medición de la efectividad de la función de seguridad, considerando activamente el nivel aceptable de riesgo, y el nivel de seguridad que prevalece en la organización, a partir de medir los componentes del riesgo y el manejo de las brechas de seguridad.</li> </ul> |

| Estado general  | Medidas correctivas   |
|---|---|
| <p><b>Gestión de la seguridad y privacidad de la información</b></p> <p><b>“Seguridad de los activos informáticos”</b></p>  |   |
| <ul style="list-style-type: none"> <li>• En mayor medida, las empresas del sector de TI son responsables de sus propias instalaciones donde se encuentra la infraestructura tecnológica para el procesamiento de información.</li> <li>• El enfoque de protección se ha centrado sobre aseguramiento de la infraestructura y no sobre el tipo de información que procesa la organización.</li> <li>• Se identifica un avance considerable en mecanismos de protección relativos a redes de telecomunicaciones, plataformas y equipos de usuario final.</li> <li>• Los esfuerzos actuales de controles de seguridad, no se han desarrollado con requerimientos de privacidad.</li> <li>• La premisa de la selección y características de los mecanismos de control de</li> </ul> | <ul style="list-style-type: none"> <li>• Realizar una revisión detallada sobre las características de sus instalaciones de cómputo para asegurarse que cumplen con los requerimientos de la industria (según estándares aplicables)</li> <li>• En su defecto, solicitar al proveedor de las instalaciones de cómputo, que entregue periódicamente resultados de revisiones o evaluaciones de sus instalaciones.</li> <li>• Desarrollar una estrategia de aseguramiento y privacidad de la información basada en controles preventivos, de detección y correctivos, cuya implementación considere políticas, procedimientos y mecanismos técnicos, que ayuden al cumplimiento de la LFPDPPP y ayuden a alcanzar el nivel de operación requerido</li> </ul> |

| <b>Estado general</b>  | <b>Medidas correctivas</b>   |
|--|--|
| <p>seguridad, es la subjetividad/experiencia del personal responsable de la función de seguridad en la organización.</p> <ul style="list-style-type: none"> <li>Existen esfuerzos incipientes sobre el monitoreo preventivo de seguridad a partir de la generación, preservación y explotación, por lo que no se contribuyen a generar métricas de la efectividad de la función de seguridad.</li> </ul> | <p>por la organización (las especificaciones recomendadas para estos controles se pueden encontrar en el "Marco práctico referencial de mecanismos de control de gestión de seguridad y privacidad de la información"</p> <ul style="list-style-type: none"> <li>Desarrollar un componente de medición de la efectividad de la función de seguridad de la información. En primera instancia puede considerar capacidades de autorregulación y gradualmente revisiones por terceros.</li> </ul> |
| <p><b>Tratamiento de datos en el denominado cómputo en la nube</b></p>   |  |
| <ul style="list-style-type: none"> <li>Las organizaciones que ofrecen o consumen servicios de cómputo en la nube, consideran sus implicaciones dentro de su marco normativo de seguridad y privacidad.</li> <li>Sin embargo, los proveedores de estos servicios de cómputo en la nube no tienen un conocimiento</li> </ul>   | <ul style="list-style-type: none"> <li>Desarrollar una estrategia de aseguramiento y privacidad de la información basada en controles preventivos, de detección y correctivos, cuya implementación considere políticas, procedimientos y mecanismos técnicos, que ayuden al cumplimiento de la LFPDPPP y ayuden a alcanzar el</li> </ul>   |

| Estado general  | Medidas correctivas   |
|---|---|
| <p>pleno sobre las implicaciones de la regulación de privacidad sobre la gestión de sus servicios desde el punto de vista de operación, nivel de servicio y legal ante una brecha o desviación de los acuerdos contractuales.</p> | <p>nivel de operación requerido por la organización (las especificaciones recomendadas para estos controles se pueden encontrar en "Marco práctico referencial de mecanismos de control de gestión de seguridad y privacidad de la información".</p> <ul style="list-style-type: none"> <li>Las organizaciones deben incluir a las áreas comerciales, de operación y jurídicas en la definición de los roles y responsabilidades de seguridad y privacidad, con una asignación puntual de la determinación de acuerdos y términos legales, niveles de servicio y desviaciones relativas a brechas de seguridad e incidentes con proveedores, socios de negocio y clientes.</li> </ul> |

**III.3 Políticas Públicas.** A la actividad f) en el rubro de Metodología de Trabajo del apartado 5 (Especificaciones Técnicas) de los Términos de Referencia, se añadió lo establecido en el inciso c) del apartado 4 (Alcance del estudio, asesoría o investigación): "c).- Las recomendaciones

y medidas correctivas deberán considerar acciones de política pública así como a nivel empresa”.

Al respecto, dicho reporte 5º pone en contexto el marco jurídico y programático que se requiere para establecer una política pública especial para el tema de la seguridad en el ámbito de las empresas de TI, que traten datos personales con el carácter de “encargados” conforme a la LFPDPPP. En este rubro se señaló que si bien es cierto que el Programa Sectorial de Economía 2007-2012 no es específico en este aspecto, sus objetivos sirven de marco para proveer mecanismos o medidas para elevar la competitividad de las empresas mediante el fomento del uso de las TI en la materia. Se comprende que este Programa no haya determinado líneas de acción exhaustivas para la economía en general, ni para la digital en lo particular, pues cuando fue emitido en mayo del 2008, México no contaba con lo que ahora es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, emitida en el 2010.

Como **políticas públicas** o esquema programático específico, que debe orientarse desde el poder público, se propusieron en este proyecto los siguientes objetivos con sus respectivas líneas de acción:

**Objetivo General.** Impulsar el conocimiento de buenas prácticas nacionales e internacionales en materia de seguridad de datos para el sector de las TI.

**Objetivo 1.** Generalizar el uso de buenas prácticas en materia de seguridad de datos personales en el sector de TI, para poder brindar certeza a las empresas y particulares que las subcontraten bajo la figura de encargado prevista en la LFPDPPP.

**Objetivo 2.** Desarrollar habilidades sobre prácticas nacionales e internacionales en materia de seguridad de datos para personas físicas o morales relacionadas con el sector de las TI, que operen como

encargados en el tratamiento de datos personales en posesión de los particulares.

**Objetivo 3.** Promover recomendaciones y medidas correctivas para una efectiva práctica de medidas de seguridad en protección de datos personales en las empresas de TI por parte de las personas físicas o morales, que operen como encargados en el tratamiento de datos personales en posesión de los particulares.

Se requiere señalar que el éxito de las Políticas Públicas que se promuevan para impulsar el conocimiento de buenas prácticas nacionales e internacionales en materia de seguridad de datos personales para el sector de las TI, con los objetivos descritos con antelación y sus líneas de acción correspondientes, radica en que exista infraestructura humana, organizativa y material; que se cuente con recursos financieros; y sobre todo, que los destinatarios de las mismas, en este caso los particulares que fungen como encargados en el tratamiento de datos personales, sean adecuadamente incentivados a alinearse a estándares, buenas prácticas y, principalmente, a las expectativas institucionales de la industria y de los titulares de los datos.

Al efecto, las dependencias deberán considerar en su respectivo Presupuesto de Egresos anual, partidas para Promover dentro de su sector de influencia conforme a la Ley Orgánica de la Administración Pública Federal, el uso de buenas prácticas en materia de seguridad de datos personales en el sector de TI, para poder brindar certeza a las empresas y particulares que las subcontraten bajo la figura de encargado prevista en la LFPDPPP, en coadyuvancia con el IFAIPD; así como para establecer una unidad administrativa que atienda los asuntos de protección de datos personales en posesión de los particulares desde un punto de vista sectorial.

Como **instrumentos de política**, se han recomendado –entre otras- los siguientes: un Sistema Nacional de Información de normas, estándares y buenas prácticas en materia de seguridad de datos personales en el sector de TI, cuyo objetivo será orientar e informar a las empresas y particulares que subcontraten servicios de tratamiento bajo la figura de encargado prevista en la LFPDPPP y un Inventario Nacional de empresas de TI dentro del Sistema de Información Empresarial Mexicano (SIEM).

Y finalmente, sobre el tema de los **responsables institucionales de ejecutar estas políticas públicas**, se destacó que conforme las leyes mexicanas sobre administración pública federal, son 19 instituciones públicas (Secretarías de Estado, Procuraduría General de la República y Consejería Jurídica), más la coadyuvancia del IFAIPD, las que tienen injerencia en el terreno de las regulaciones sobre privacidad. De aquí que estos 20 organismos en total, deban ser considerados como sujetos responsables de encauzar armónicamente las Políticas Públicas correspondientes.

**PROYECTO ELABORADO PARA LA CÁMARA  
NACIONAL DE LA INDUSTRIA ELECTRÓNICA, DE  
TELECOMUNICACIONES Y TECNOLOGÍAS DE LA  
INFORMACIÓN (CANIETI)**



**REALIZADO POR PIVOTAL SERVICIOS, S. DE R.L. DE  
C.V.**



**www.pivotalmexico.com**

**flor.hernandez@pivotalmexico.com**

**2011-2012**