Privacy by design para fomentar la figura del encargado

(Procesos 2013)

— 3ª entrega: Entrega Final —

Fase 3:

Esta fase contempla los siguientes elementos:

- Analizar desde el punto de vista técnico los beneficios e impactos de insertar el modelo PbD en el desarrollo e implementación de sistemas de información en las empresas. De esta forma realizar la implementación piloto del modelo de PbD en una empresa del Sector de TI.
- Emitir las recomendaciones que sirvan a responsables y encargados del tratamiento para adoptar buenas prácticas a considerar en el diseño o re-diseño de un sistema de información y garantizar así el cumplimiento normativo en protección de datos personales.

Contenido

Página

Abreviaturas

Art(s).	Artículo(s)
DOF	Diario Oficial de la Federación
FTC	Federal Trade Commission (Estados Unidos)
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LFTyR	Ley Federal de Telecomunicaciones y Radiodifusión
PbD	Privacy by Design (privacidad por diseño)
PETs	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment (Evaluación de impacto de privacidad)
RGPD	Reglamento general de protección de datos (Unión Europea)
SE	Secretaría de Economía
SEPD	Supervisor Europeo de Protección de Datos
TIC	Tecnologías de la Información y las Comunicaciones
UE	Unión Europea

Presentación

El Proyecto de Desarrollo de la Industria de las Tecnologías de la Información (PROSOFT 3.0) a cargo de la Secretaría de Economía, ha contado con el apoyo del Banco Mundial (Préstamo 7571-MX) para promover estudios que permitan desarrollar a este sector en nuestro país, aprovechando el potencial de crecimiento interno y global para los servicios de TI.

Con ese marco, a la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI) le ha correspondido ser participante en el componente *F) Fortalecimiento Institucional y mejora del marco legal, regulatorio y de políticas sectoriales*, que tiene como finalidad mejorar el marco regulatorio para fomentar el desarrollo del comercio electrónico y el sector de TI.

En particular, la CANIETI ha estado interesada en promover estudios en materia de protección de datos personales, tales como los relacionados con autorregulación y la autogestión, con el fin de promover la debida protección de datos personales en las empresas. De ahí que se haya promovido ahora el desarrollo del proyecto denominado **Privacy by Design para Fomentar la Figura del Encargado** (Procesos 2013), el cual persigue los siguientes objetivos:

a) Desarrollar un estudio que permita a las empresas, en particular a las MIPYMES del sector de TI, aprovechar y aplicar dicho modelo.
b) Entrevistar a la creadora del modelo Dra. Ann Cavoukian, o en su defecto a quien designe, para ampliar el conocimiento del modelo aplicado a las empresas, en particular a las pequeñas.
c) Concientizar a las empresas, sobre los beneficios de la privacidad por diseño y lo que ello supone para el desarrollo de una cultura de protección de datos personales.
d) Analizar casos de éxito de la aplicación del modelo y sus beneficios.
e) Realizar un proyecto piloto en una empresa del Sector de TI para implementación del modelo de PbD.

El estudio se concibió para realizarse en tres etapas:

Fase 1: Esta fase contemplará la entrega de al menos los siguientes elementos:

- Investigación y análisis a nivel internacional del concepto de privacidad por diseño (Privacy by Design, PbD),
- Análisis práctico de la privacidad por diseño desde el punto de vista de la normatividad mexicana en protección de datos, la LFPDPPP y su Reglamento.
- Realizar el análisis de las implicaciones prácticas del concepto de privacidad por diseño, con lo que ello supone para responsables y encargados del tratamiento, prestando especial atención a las empresas mexicanas del sector de TI, e interrelación del concepto con los principios v deberes de los responsables y encargados del tratamiento en la normatividad mexicana sobre protección de datos.

Fase 2: Esta fase contemplará la entrega de al menos los siguientes elementos:

- Desarrollar los contenidos para entrevistar a la precursora del PbD, la Dra. Ann Cavoukian, Comisionada de la Oficina de privacidad e información de Ontario, Canadá.
- Los contenidos de la entrevista deberán enfocarse en el desarrollo de al menos los siguientes puntos:
    - Análisis de los principios del PbD
    - Beneficios de la implementación en las empresas
    - Papel o rol de las Tecnologías de Información
    - Facilidad de implementación en las empresas
    - Casos de éxito desarrollados
    - Retos de la implementación del modelo.
- Desarrollar la entrevista, con previo acuerdo del Beneficiario y la Secretaría de Economía.

Fase 3: Esta fase contemplará la entrega de al menos los siguientes elementos:

- Analizar desde el punto de vista técnico los beneficios e impactos de insertar el modelo PbD en el desarrollo e implementación de sistemas de información en las empresas. De esta forma realizar la implementación piloto del modelo de PbD en una empresa del Sector de TI.
- Emitir las recomendaciones que sirvan a responsables y encargados del tratamiento para adoptar buenas prácticas a considerar en el diseño o re-

diseño de un sistema de información y garantizar así el cumplimiento normativo en protección de datos personales.

De estas, corresponde ahora reportar esta última tercera fase a manera de Entrega Final que condensa los hallazgos de las primeras dos etapas, para dar contexto a las recomendaciones que se esperan del proyecto. En este sentido, esta Entrega Final se divide en dos Partes: Una que retoma las Fases 1 y 2 y otra que reporta la Fase 3.

Es importante hacer notar que durante la realización de este proyecto, el consultor tuvo en todo momento la orientación de la CANIETI, así como de la Dirección General de Innovación, Servicios y Comercio Interior y de su Dirección de Economía Digital, ambas adscritas de la Subsecretaría de Industria y Comercio de la Secretaría de Economía.

En particular, esta firma consultora a cargo del proyecto agradece la colaboración del Mtro. Miguel Recio Gayo, quien es Egresado de la Facultad de Derecho de la Universidad Carlos III de Madrid (España) y maestro en Derecho de la Propiedad Intelectual por la George Washington University Law School (Estados Unidos).

Durante sus más de 12 años de actividad profesional ha trabajado como abogado especializado en Derecho de las Tecnologías de la Información y las Comunicaciones (TIC), asesor legal para Latinoamérica en Business Software Alliance (BSA) en Washington, D.C. y actualmente dirige Global Data Protection Consulting en Madrid, una firma de servicios jurídicos y consultoría especializada en Derecho de las TIC.

Recio cuenta con una amplia experiencia asesorando a empresas de diferentes sectores de actividad y gobierno. En México, ha asesorado al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) en diferentes ocasiones y es autor de diversas publicaciones en materia de protección de datos personales.

PRIMERA PARTE

Marco Teórico

1. Introducción

La privacidad por diseño (en inglés, *privacy by design*, PbD) es, sin duda alguna, una necesidad para las organizaciones, públicas o privadas, que tratan datos personales ya sea como responsables o encargados del tratamiento.

Específicamente en el sector privado, en la actualidad ya no es posible pensar en una organización, con independencia de su tamaño o mercado, que no haga uso de las Tecnologías de la Información y las Comunicaciones (en adelante, TIC) para el tratamiento de datos personales. Es decir, en la actualidad, las organizaciones tratan datos personales para el desarrollo de su negocio y lo hacen a través del uso de tecnologías de la información.

Unido a lo anterior, los datos personales son, en la actualidad, uno de los principales activos de las organizaciones y un recurso necesario para el avance de la economía digital. Ahora bien, que los datos personales sean vistos como un activo o recurso no debe hacernos perder de vista que se refieren a personas físicas que tienen reconocido un derecho fundamental a la protección de sus datos personales, de manera que el tratamiento de los mismos debe hacerse con apego a la normatividad aplicable, general y específica o sectorial.

Al respecto, la privacidad por diseño, que fue creada por la Dra. Ann Cavoukian y reconocida como estándar global de privacidad en octubre de 2010 a través de la Resolución sobre Privacidad por Diseño[1], adoptada durante la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, tiene por objeto servir como aproximación de manera que los nuevos modelos o prácticas de negocio, las especificaciones tecnológicas y las infraestructuras físicas incluyan principios de privacidad de manera que respeten el derecho fundamental a la protección de datos personales.

El hecho de que la privacidad o la protección de datos personales esté embebida, es decir, sea un aspecto a tomar en consideración desde el diseño o fase inicial de una práctica de negocio o el desarrollo de un sistema de información, es una garantía que debe permitir a los responsables y encargados del tratamiento conseguir una ventaja competitiva.

[1] Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners. Disponible, en inglés, en el siguiente vínculo electrónico http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

Por otra parte, los principios fundamentales que forman parte de la privacidad por diseño deben ponerse en relación con los principios y deberes de protección de datos personales previstos en la normatividad general en la materia, específicamente la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[2] (en adelante, LFPDPPP) y su Reglamento[3].

Es así que los sujetos obligados que tienen que cumplir con dicha normatividad, los responsables y encargados del tratamiento, deben tomar en consideración la privacidad por diseño como un diferenciador a la hora de desarrollar sus prácticas de negocio o sus sistemas de información, ya que, en determinados casos, el uso de las TIC permite llevar a cabo un tratamiento de los datos personales de una manera desconocida hasta el momento. Basta pensar en los retos que se plantean para la privacidad y la protección de datos personales, tales como el *big data*, la Internet de las cosas (en inglés, *Internet of Things*, IoT) u otros retos que estén por llegar.

Se trata, por tanto, de que la privacidad por diseño, alineada con el negocio desde el momento mismo de establecer un modelo de negocio o plantear el desarrollo de un sistema de información, permita el desarrollo de mejores prácticas que sirvan para generar la confianza necesaria por los consumidores o usuarios de los bienes o servicios que sean ofrecidos por los responsables y, en su caso, en los que intervengan encargados del tratamiento.

Nótese que la figura del encargado del tratamiento no es secundaria, sino que en muchas ocasiones dichos encargados son quienes tratan los datos personales y que los responsables se centran en otras partes de su negocio sin llevar a cabo dicho tratamiento, y también que dichos encargados pueden ser quienes proporcionen bienes o servicios que sean utilizados por los responsables para el tratamiento de datos personales.

Cabe señalar que en este entregable se presta especial atención al concepto de privacidad por diseño, lo que supone partir de la definición del mismo para, a continuación, tomar en consideración los siete (7) principios fundamentales que la integran. Además, ya que se trata de un principio internacional, se analizan referencias normativas relevantes así como las guías u otros instrumentos que,

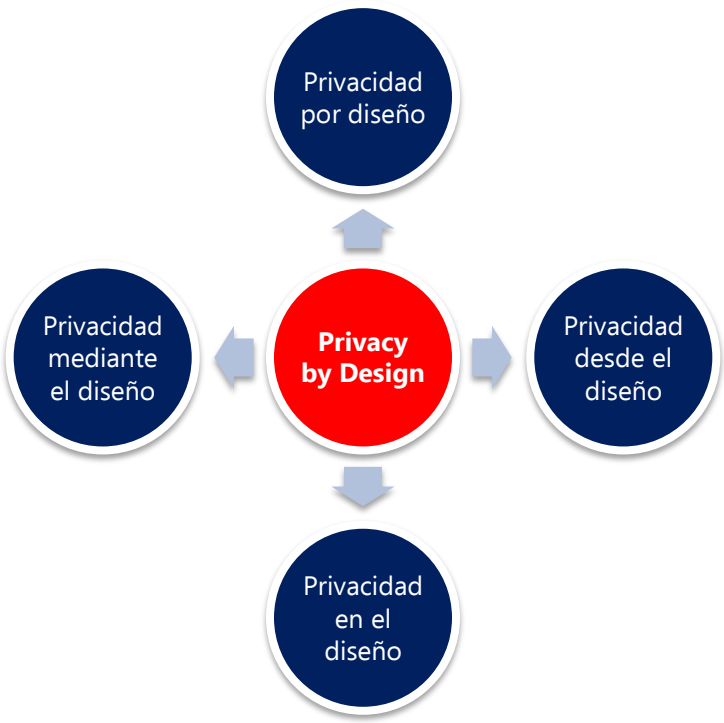
[2] Publicada en el Diario Oficial de la Federación de 5 de julio de 2010.
[3] Publicado en el Diario Oficial de la Federación de 21 de diciembre de 2011.

hasta la fecha, han sido desarrollados por diferentes autoridades garantes de protección de datos alrededor del mundo. Dicho análisis permite, por último, interrelacionar los principios fundamentales de la privacidad por diseño con la normatividad general sobre protección de datos personales de manera que sirva como referencia para los sujetos obligados, especialmente, para los encargados del tratamiento.

2. Concepto de privacy by design (PbD)

2.1 Definición

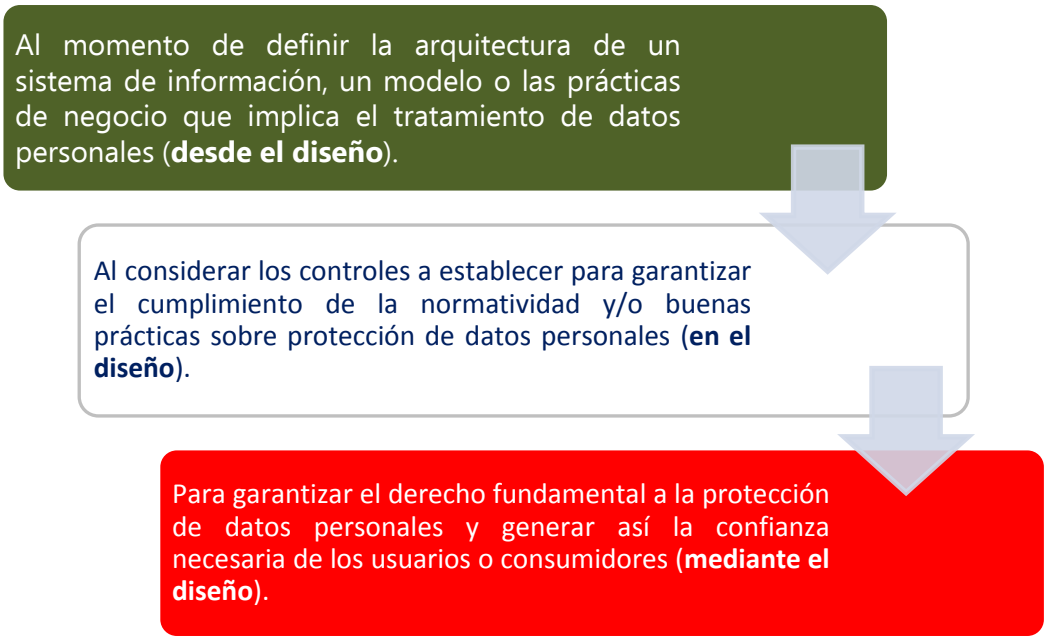
Antes de proporcionar una de definición de este concepto, es necesario señalar que la traducción al español del término *"privacy by design"* puede dar lugar a diversas posibilidades, considerándolas como sinónimos y pudiendo señalar al respecto las siguientes:



Se trata de una cuestión que se plantea habitualmente en diferentes ámbitos, no solo en materia de términos jurídicos y/o tecnológicos, que en ningún caso debe ser un obstáculo o distracción para poner foco en la cuestión central que es que la privacidad por diseño, o el sinónimo que se quiera emplear en su caso, tiene por objeto asegurar la protección de datos personales a través de siete (7) principios fundamentales que deben garantizarse en el diseño de prácticas de negocio o sistemas de información que implican, en cualquier caso, el uso de las Tecnologías de la Información y las Comunicaciones (TIC).

Insistimos en que todas estas traducciones del mismo término pueden considerarse como equiparables, ya que la privacidad por diseño implica que la

protección de datos personales sea tomada en consideración, como factor o cuestión clave:



Con carácter general, la privacidad por diseño puede definirse como un concepto que, a través de los siete (7) principios fundamentales que veremos, tiene el propósito de especificar la protección que confieren los marcos regulatorios en materia de protección de datos personales y privacidad.

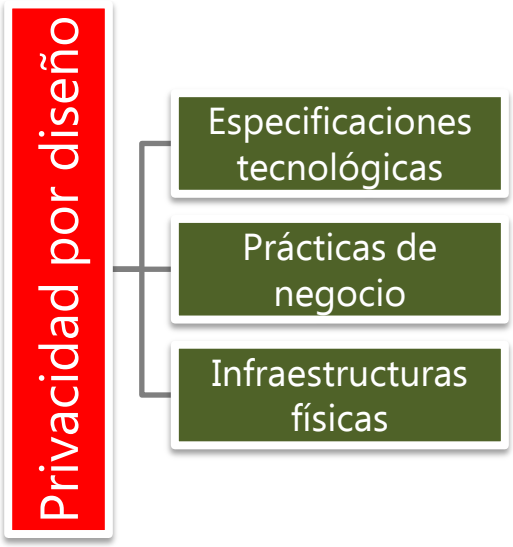
Citando al respecto a la Dra. Cavoukian, la privacidad por diseño es un concepto que desarrolló en los años 90 para dar respuesta a *"los efectos siempre crecientes y sistemáticos de las Tecnologías de la Información y las Comunicaciones, y de los sistemas de datos en red a gran escala"*[4].

Es decir, la privacidad por diseño permite especificar el cumplimiento de los principios de la protección de datos personales a través de la inclusión de controles desde el momento mismo en que se diseña un modelo de negocio, un sistema de información o una infraestructura física, de manera que ello permite garantizar el derecho fundamental a la protección de datos personales, ya que los sujetos obligados actuarán desde el inicio con plena sujeción a la normatividad

[4] Véase el documento relativo a Los 7 principios Fundamentales, en español, en el siguiente vínculo electrónico http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf

sobre protección de datos personales. A su vez, esto supone minimizar los riesgos por incumplimiento de la normatividad sobre protección de datos personales.

Esta concepción de la privacidad por diseño, como aproximación a la necesidad de proteger la privacidad y protección de datos personales, se despliega en tres ámbitos, que son los siguientes:



Es así que, tal y como se indica en el Dictamen Supervisor Europeo de Protección de Datos acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad[5], la privacidad por diseño puede suponer diferentes acciones, dependiendo del caso o la aplicación concretos.

Por ejemplo, en algunos casos puede obligar a eliminar o reducir datos personales (minimización del tratamiento) o evitar tratamientos innecesarios o no deseados. En otros casos, la privacidad por diseño puede dar lugar a que se ofrezcan herramientas para aumentar el control que tienen las personas sobre sus datos personales. Estas medidas se deberían tener en cuenta al definir los estándares o las mejores prácticas. También se podrían incorporar en la arquitectura de los sistemas de información y comunicación, o en la organización estructural de las entidades que tratan datos personales.

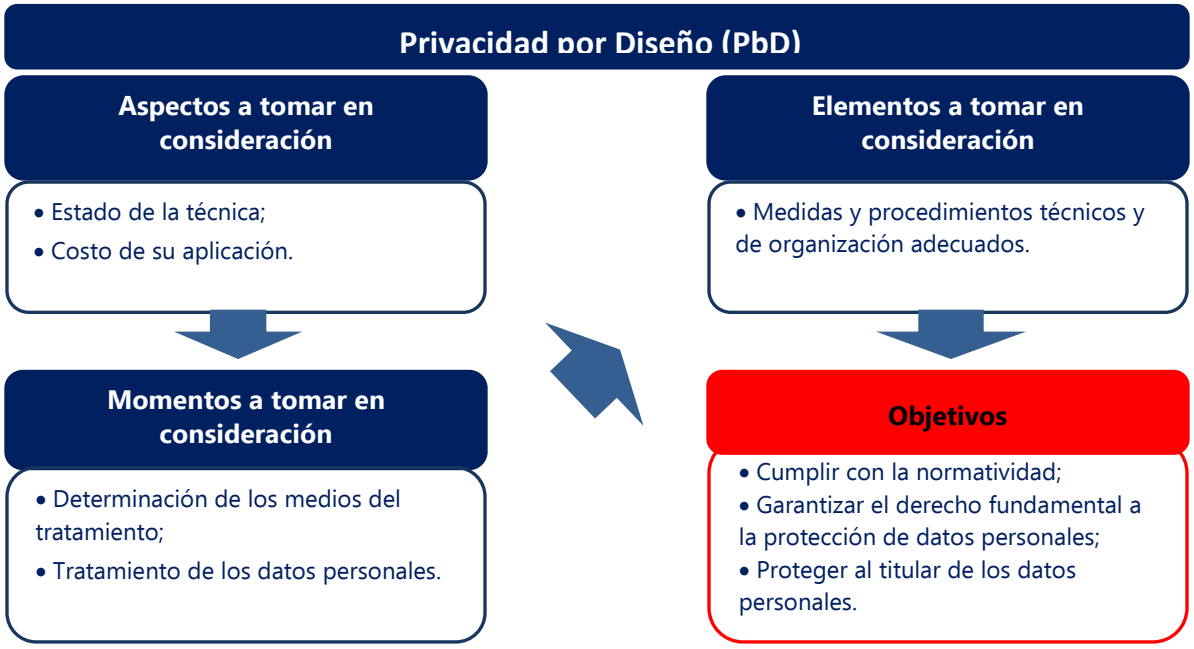
A nivel internacional, si buscamos una clara referencia a la definición de privacidad por diseño, es recomendable tomar en consideración la Recomendación relativa a

[5] Publicado en el Diario Oficial de la Unión Europea serie C, número 280, de 16 de octubre de 2010.

los preparativos para el despliegue de los sistemas de contador inteligente[6], ya que en el apartado I.3.d) se define el concepto de protección de datos desde el diseño de la siguiente manera:

> *"aplicación, teniendo en cuenta el estado de la técnica y el coste de dicha aplicación, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, de las medidas y los procedimientos técnicos y de organización adecuados para que el tratamiento satisfaga los requisitos de la Directiva 95/46/CE y garantice la protección de los derechos del interesado."*

Si bien la definición se encuentra en una Recomendación[7], es relevante ya que hace referencia a varios elementos esenciales a tomar en consideración cuando se trata el concepto de privacidad por diseño. Dichos elementos son los siguientes:

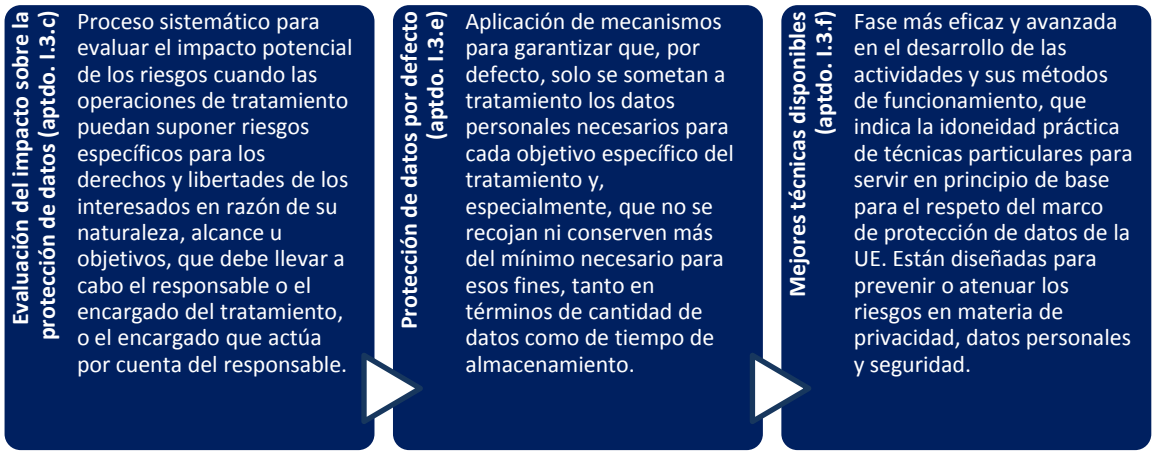


[6] Publicada en el Diario Oficial de la Unión Europea serie L, número 73, de 13 de marzo de 2012. Disponible, en español, en el vínculo electrónico http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:ES:PDF

[7] En el ámbito de la Unión Europea, una Recomendación es un acto jurídico a través del que las instituciones de la Unión, en este caso la Comisión, puede expresarse de forma no vinculante para los destinatarios. Es decir, a través de la Recomendación no se establecen obligaciones legales para los destinatarios de las mismas. Para más información sobre los actos jurídicos de la Unión Europea puede verse Dr. Klaus-Dieter Borchardt, El ABC del Derecho de la Unión Europea, 2011. Disponible, en español, en el vínculo electrónico http://bookshop.europa.eu/es/el-abc-del-derecho-de-la-uni-n-europea-pbOA8107147/downloads/OA-81-07-147-ES-C/OA8107147ESC_002.pdf?FileName=OA8107147ESC_002.pdf&SKU=OA8107147ESC_PDF&CatalogueNumber=OA-81-07-147-ES-C

El concepto de privacidad por diseño está relacionado, a su vez, con los conceptos de evaluación del impacto sobre la privacidad o protección de datos (en inglés, *Privacy Impact Assesment*, PIA); protección de datos por defecto (en inglés, *privacy by default*) y mejores técnicas disponibles (en inglés, *Privacy Enhancing Technologies*, PETs).

Desde un punto de vista normativo, dichos conceptos no se encuentran definidos en la normatividad mexicana, de manera que es posible hacer referencia a las definiciones dadas a nivel internacional en la Recomendación relativa a los preparativos para el despliegue de los sistemas de contador inteligente[8], que son las siguientes:



Es decir, la privacidad por diseño está interrelacionada con estos otros conceptos, ya que a la misma se llega evaluando el impacto que tiene para la privacidad unas prácticas de negocio o un sistema de información, y estableciendo mecanismos de protección de datos personales por defecto a través de las mejores técnicas disponibles. La interrelación entre los cuatro conceptos es clara y debe ser tomada en consideración por los sujetos obligados que tienen que cumplir con los principios y deberes de la protección de datos personales que les son exigibles.

En definitiva, la privacidad por diseño implica adoptar medidas para garantizar los principios de la protección de datos, deberes (seguridad y confidencialidad), así como derechos ARCO desde el inicio, incluso antes de tratar datos personales. De esta manera, por un lado, se protege el derecho fundamental a la protección de datos personales y, por otro lado, se minimiza el riesgo por incumplimiento de la normatividad sobre protección de datos personales.

[8] Ya citada.

2.2. Alcance

No cabe duda de que los datos personales son necesarios, y por tanto, activos, para cualquier empresa y, especialmente, para aquellas tecnológicas o con base tecnológica. Dichos datos personales tienen que tratarse, en el caso de México, conforme a la normatividad sobre protección de datos personales de manera que se consiga *"su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas"* (art. 1 de la LFPDPPP).

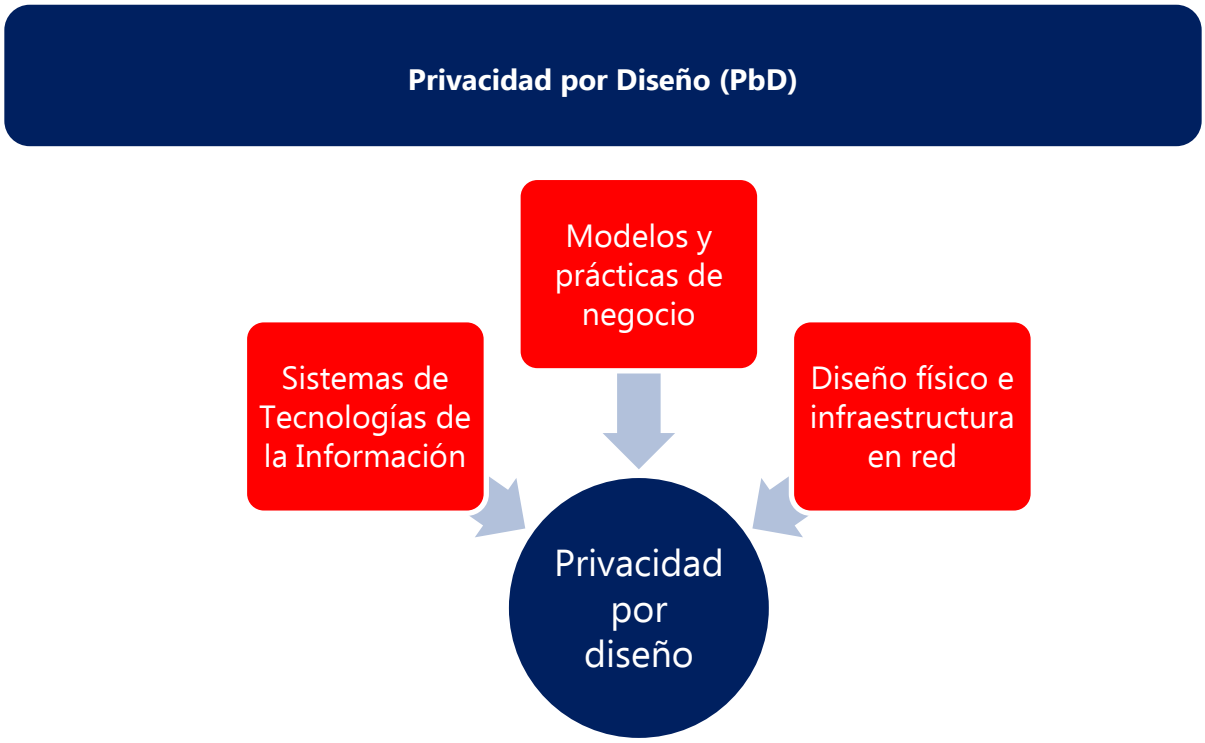
Desde una base de datos de clientes o recursos humanos, pasando por aplicación (en inglés, *´app´*), hasta una red social, son algunos ejemplos de casos en los que la privacidad por diseño es fundamental ya que, en caso contrario, podrían darse situaciones en las que un mal diseño o una gestión inadecuada de los datos personales dé lugar, por una parte, a una sanción en caso de que se verifique un incumplimiento de la normatividad sobre protección de datos personales y, por otra parte, al propio fracaso del negocio ya que los controles necesarios no fueron considerados en el diseño del sistema de información, producto o servicio correspondiente.

En relación con la obligación de garantizar el derecho fundamental a la protección de datos personales, la privacidad por diseño desempeña un papel relevante. Es así que, a pesar de que no se trata de un principio que se encuentre expresamente previsto en la normatividad mexicana sobre protección de datos personales, a la privacidad por diseño se llega mediante la adopción de medidas proactivas y preventivas de manera que permite a los responsables y encargados del tratamiento cumplir con sus los principios y los deberes así como reducir el riesgo que supone y conlleva todo tratamiento de datos personales.

Es decir, tanto el responsable como el encargado del tratamiento, en sus respectivos ámbitos de actuación, tienen la obligación de proteger al titular de los datos personales por lo que se refiere a su derecho fundamental a la protección de datos personales, de manera que deben tomar en consideración la privacidad por diseño como una medida proactiva y preventiva a través de la que puedan minimizar el riesgo derivado del tratamiento de los datos personales.

Desde el punto de vista del alcance de aplicación de la privacidad por diseño, se encuentra presente en todos los ámbitos de la actividad de una empresa u

organización, ya que tal y como se representa en el siguiente gráfico, aquella incumbe a:



En definitiva, la privacidad por diseño, además de asegurar la protección de datos personales, debe ser tomada en consideración como un elemento fundamental para conseguir también otros objetivos al mismo tiempo, tales como:

— Responsable y encargado del tratamiento

Lo anterior implica que tanto el responsable como el encargado del tratamiento tengan que adoptar medidas con la finalidad de garantizar el derecho fundamental a la protección de datos personales.

Al respecto, el responsable tiene la obligación de velar por el cumplimiento de los principios y deberes en el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, así como por los tratamientos que lleve a cabo un encargado por cuenta de aquél.

Incluso cuando el encargado del tratamiento ofrece productos o servicios que pueden ser utilizados por el responsable para el tratamiento de datos personales, es necesario que se garantice el cumplimiento de los principios y deberes previstos en la normatividad sobre protección de datos personales. Es decir, la privacidad por diseño, con la finalidad de garantizar el derecho fundamental a la protección de datos personales, debe ser la ruta a seguir por el encargado del tratamiento.

Un claro ejemplo de esta última situación se encuentra en el Reglamento de la LFPDPPP, y es el relativo a los proveedores de cómputo en la nube (en inglés, *´cloud computing´*). En concreto, conforme al inciso a) de la fracción I, del artículo 52 del Reglamento, el proveedor de servicios de cómputo en la nube tiene que cumplir, al menos, con *"[t]ener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento."*

Se trata de un caso en el que el proveedor de servicios, que será considerado como un encargado del tratamiento si trata datos personales por cuenta del responsable, y con independencia de si está establecido en México o en otro país, tiene que proporcionar un servicio que permita garantizar los principios y deberes aplicables en la normatividad mexicana sobre protección de datos personales.

Además de lo anterior, resulta claro que entre las obligaciones del encargado del tratamiento se encuentran tanto las que hacen referencia a cumplir con los principios de la protección de datos personales como aquellas que se refieren a los deberes. Al respecto, tomando en consideración el artículo 50 del Reglamento de la LFPDPPP, es posible organizar dichas obligaciones tomando en consideración los principios y deberes de la protección de datos personales de la siguiente manera:

Art. 50	Principios	Deberes
Fracc. I	Tratar únicamente los datos personales conforme a las instrucciones del responsable.	
Fracc. II	Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.	—
Fracc. III	—	Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables.
Fracc. IV	—	Guardar confidencialidad respecto de los datos personales tratados.
Fracc. V	Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable,	—

	siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.	
Fracc. VI	Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.	—

Lo anterior implica que la privacidad por diseño deba ser considerada tanto por el responsable como el encargado del tratamiento en cualquier acción que realicen y que implique un tratamiento de datos personales.

En el caso del responsable, este debe asegurarse de que si encomienda a un encargado el tratamiento de los datos personales, se haga conforme a los acuerdos que ambos alcancen y que, en su caso, los datos personales sean tratados en sistemas de información o a través de servicios que cumplan con las garantías necesarias y adecuadas. Por tanto, la privacidad por diseño debe ser también una cuestión a considerar cuando el responsable acude a un encargado del tratamiento.

Por otra parte, un encargado de tratamiento que desarrolla productos o servicios, por ejemplo, un centro de asistencia telefónica (en inglés, *call center*), un sistema de gestión de relación con los clientes (en inglés, *Customer Relationship Management*, CRM), debe considerar embeber principios de la privacidad por diseño de manera que posteriormente sirvan como controles para garantizar el cumplimiento de la normatividad sobre protección de datos personales.

Esto supone, a la vista de la normatividad general aplicable, aplicar desde el inicio los principios y deberes de la protección de datos personales, conforme a lo previsto en la LFPDPPP y su Reglamento.

Es decir, desde el punto de vista de quien desarrolla productos o servicios de TI que posteriormente van a ser utilizados por un responsable, para tratar datos personales de sus clientes que son personas físicas, y por estas últimas, es necesario garantizar que dichos productos o servicios cumplan con la normatividad sobre protección de datos personales desde la fase inicial de su diseño.

Lo anterior ayudará al responsable del tratamiento a cumplir con sus obligaciones, debiendo tomar en consideración que en ocasiones el encargado del tratamiento puede conocer mejor que el propio responsable cómo cumplir con la normatividad. Por ejemplo, sería posible pensar en un encargado del tratamiento que desarrolla un software que va a ser utilizado por los responsables y que tienen la posibilidad de alojar o almacenar los datos personales que recaben en los servidores del encargado del tratamiento o que este les preste un servicio de asistencia técnica sobre dicho software que implique el acceso a los datos personales que se registran en las bases de datos. En estos casos, el encargado del tratamiento habrá desarrollado un software que tiene que cumplir con la normatividad sobre protección de datos personales aplicable y que, incluso podría ser utilizada por responsables del tratamiento que pudieran carecer de los conocimientos necesarios en materia de protección de datos personales.

Otro ejemplo podría ser un encargado del tratamiento que también desarrolle un software para atender el ejercicio de derechos de acceso, rectificación, cancelación y oposición por los responsables del tratamiento, de manera que el mismo debería incluir la privacidad por diseño desde el principio. En este caso, el encargado del tratamiento podría acceder a las bases de datos o incluso atender el ejercicio de los derechos en representación, es decir, por cuenta de los responsables.
Por lo que se refiere a los titulares de los datos personales que son objeto de tratamiento, es necesario tener presente que, en ocasiones, estos pueden desconocer el significado y alcance de su derecho fundamental, de manera que desarrollar los productos o servicios de los que vayan a hacer uso conforme a la privacidad por diseño les ayudará a saber cómo proteger sus datos personales, generando así la confianza necesaria en el uso de las TI.

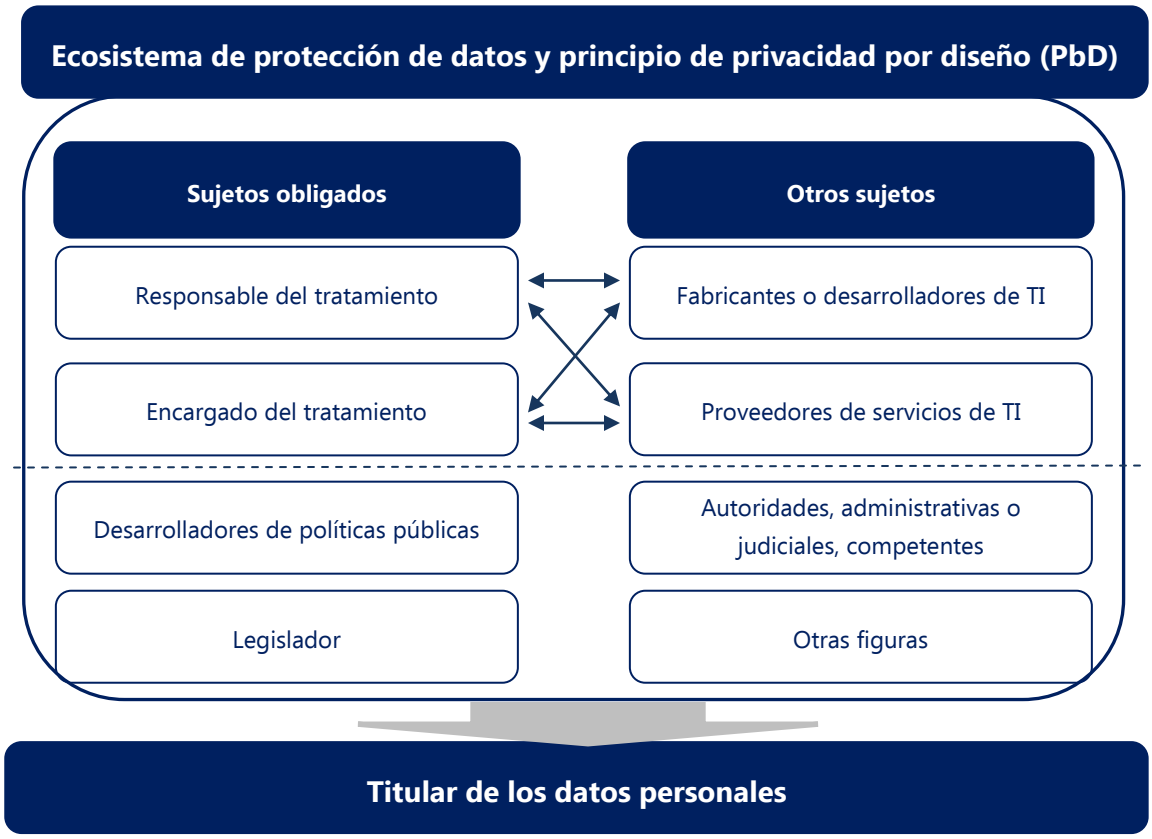
— Otras figuras

Además del responsable y encargado del tratamiento, que son las figuras principales ya que son los sujetos obligados en virtud de la normatividad sobre protección de datos personales, hay otras figuras que también tienen alguna responsabilidad en relación con el modelo de privacidad por diseño debido a su relevancia en el ecosistema de protección de datos personales. Entre dichas figuras, cabe hacer referencia específicamente a los fabricantes o desarrolladores de TI así como los proveedores de servicios de TI cuando no sean responsables o encargados del tratamiento.

Estas figuras deben adoptar igualmente la privacidad por diseño en el desarrollo de productos o servicios, ya que si bien puede que no traten datos personales porque sean los responsables y, en su caso, encargados del tratamiento quienes hagan uso de los mismos, dichos productos o servicios servirán para tratar datos personales o, específicamente, consistirán en el tratamiento de dichos datos personales.

Lo anterior implica que el responsable y el encargado del tratamiento deban tomar también en consideración que los productos o servicios de los que hagan uso o a través de los que traten datos personales cumplan con dicho modelo de privacidad por diseño, con la finalidad de garantizar el derecho fundamental a la protección de datos personales.

En definitiva, estas otras figuras también son relevantes al momento de considerar el cumplimiento de los principios y deberes de la protección de datos personales, ya que los productos o servicios que proporcionen, en la medida en que sirvan para o impliquen el tratamiento de datos personales, deben aplicar el modelo de privacidad por diseño. De esta manera, el ecosistema de protección de datos personales, por lo que se refiere específicamente a la privacidad por diseño, podría ser representado de la siguiente manera:



Nótese que tanto el responsable como el encargado del tratamiento pueden ser, por una parte, fabricantes o desarrolladores de productos o servicios de TI y, por otra parte, usuarios de los mismos de manera que a su vez los utilizan para tratar datos personales de los titulares que, a su vez, son consumidores o usuarios de los bienes o servicios correspondientes.

En particular, quienes desarrollan tecnología, ya sea como responsables o encargados del tratamiento, deben tomar en especial consideración que dicha tecnología incluya la privacidad por diseño en los productos o servicios correspondientes. Por ejemplo, los desarrolladores de servicios basados en la nube, que sean considerados a su vez como encargados del tratamiento, que se pongan a disposición de responsables del tratamiento y encargados del tratamiento, deben considerar que la privacidad por diseño ayudará a los usuarios de sus servicios a garantizar el cumplimiento, además de cumplir ellos mismos con los principios y deberes previstos en la normatividad sobre protección de datos personales.

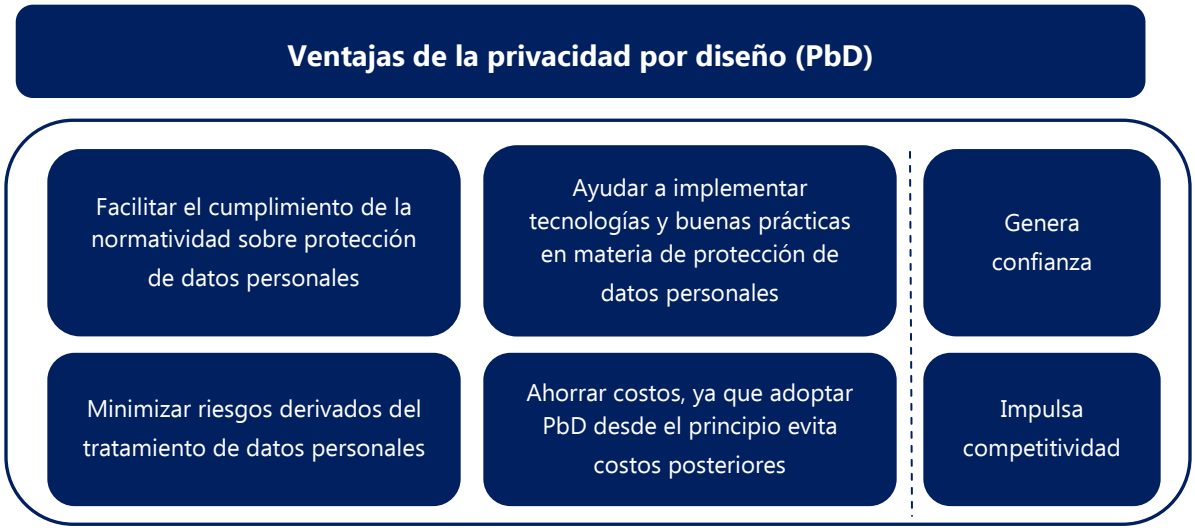
Tal y como señalamos, la privacidad por diseño tiene implicaciones para las diferentes partes que interactúan en un ecosistema de protección de datos personales, ya que quienes desarrollan tecnología o prestan servicios de TI, quienes tratan datos personales como sujetos obligados y los titulares de los datos personales, verán que aquella les ayuda a encontrar el necesario equilibrio que permita alinear los objetivos lícitos y legítimos de una organización y el respeto al derecho fundamental a la protección de datos personales.

No obstante, la privacidad por diseño, cuando es aplicada por un sujeto obligado, tiene implicaciones también para otras partes interesadas. Entre estas últimas es posible citar, por ejemplo, a las autoridades de protección de datos, ya sea el IFAI como autoridad garante o las autoridades reguladoras en cada caso. Resulta claro que dichas autoridades, especialmente el IFAI, tomarán en consideración la adopción por los sujetos obligados de medidas en relación con la privacidad por diseño, ya que esta puede permitir en su caso dar cumplimiento a la adopción de buenas prácticas, tanto desde un punto de vista proactivo como preventivo, lo que sin duda es un factor que impulsa el cumplimiento normativo, reduciendo así el riesgo de incumplimiento.

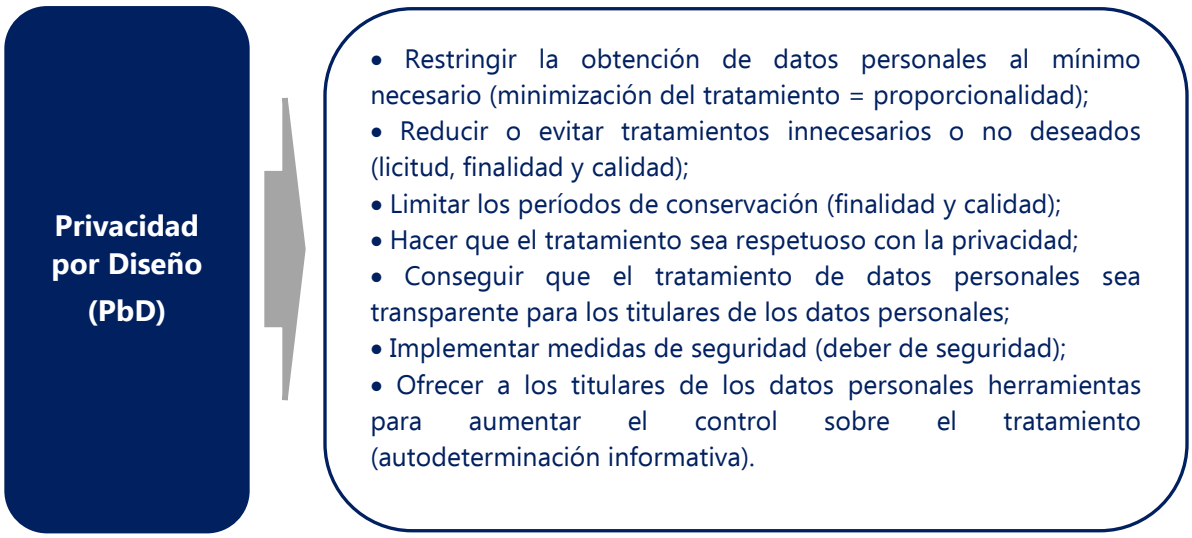
Por último, la privacidad por diseño es también una cuestión que involucra a otras partes interesadas, tales como los desarrolladores de políticas públicas o, incluso, a los legisladores u operadores jurídicos que tienen que aplicar y/o interpretar la normatividad. En todos los casos se trata de que dichas partes interesadas, en el desempeño de su correspondiente papel, aporten lo necesario para que la privacidad por diseño sea un instrumento o detonador que permita garantizar la protección de datos personales.

— Ventajas de la privacidad por diseño

Además de los objetivos que pueden conseguirse a través de la implementación del modelo de privacidad por diseño en cualquier sistema de información o modelo de negocio que implique el tratamiento de datos personales, es posible señalar algunas ventajas a las que puede dar lugar tomar en consideración la privacidad por diseño en cualquier acción que se lleve a cabo por un sujeto obligado, ya sea responsable o encargado del tratamiento, y que son las siguientes:

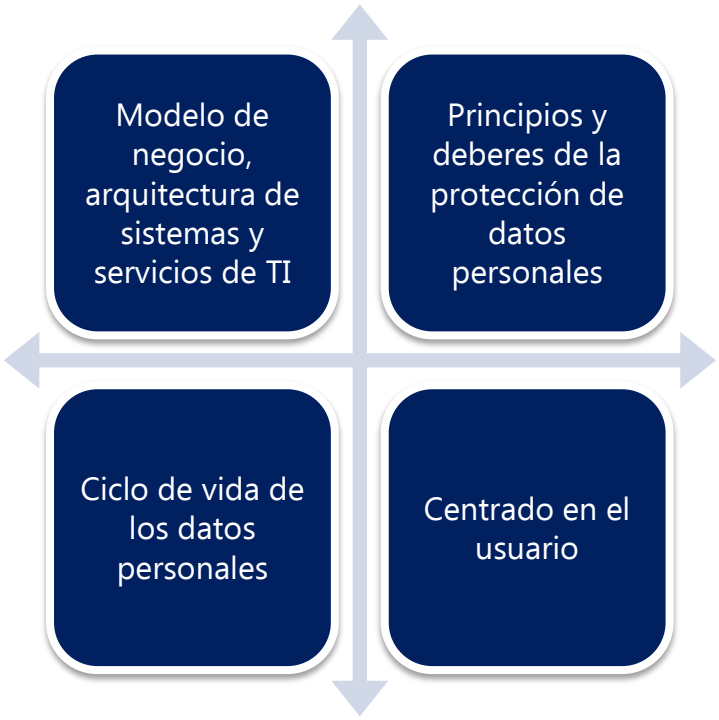


En cuanto al cumplimiento de los principios y deberes de la protección de datos personales, al implementar la privacidad por diseño desde el inicio, ya sea tomándola en consideración en un modelo de negocio, en el diseño de un sistema de información o en el desarrollo de un producto o servicio de TI, con carácter general cabe señalar lo siguiente:



Como principio a implementar tanto en la definición de la arquitectura de un sistema de TI, el funcionamiento y la gestión de aplicaciones y sistemas de información o en un modelo de negocio, la privacidad por diseño abarca todas las etapas del ciclo de vida de los datos personales que son tratados.

Además, implica a todas las áreas y a todos los sujetos, ya sean obligados o tengan alguna responsabilidad en el desarrollo de productos o servicios tecnológicos que impliquen el tratamiento de datos personales o que se utilicen para tratar datos personales. Gráficamente, el alcance de la privacidad por diseño puede ser representado de la siguiente manera:



2.3 Contenido: los 7 principios fundamentales

La privacidad por diseño (PbD) se basa en 7 principios fundamentales que son los siguientes:

Los principios fundamentales de la privacidad por diseño, a pesar de que esta no es un principio expreso de la normatividad sobre protección de datos personales en México, pueden ponerse en relación con los principios y deberes de la misma.

Se trata, por tanto, de poner en relación los principios fundamentales con los principios y deberes en materia de protección de datos personales, recordando que conforme a los artículos 6, 19 y 21 de la LFPDPPP y 9 del Reglamento, son los siguientes:

Principios de la protección de datos	Deberes de la protección de datos
Licitud	**Seguridad**
Consentimiento	**Confidencialidad**
Información	
Calidad	
Finalidad	
Lealtad	
Proporcionalidad	
Responsabilidad	

A continuación se listan cada uno de dichos principios y se relacionan con la normatividad general sobre protección de datos personales, es decir, la LFPDPPP y su Reglamento:

Principios fundamentales de la PbD	Principio	Normatividad sobre protección de datos personales
Proactivo y preventivo	Responsabilidad	Velar por el cumplimiento de los principios de la protección de datos, adoptando las medidas necesarias para su aplicación.
Configuración predeterminada	Todos los principios y deberes	Deber de cumplir con los principios rectores de la protección de datos personales.
Privacidad en el diseño		
Funcionalidad total (todos ganan)		
Seguridad Extremo-a-Extremo	Seguridad	Medidas de seguridad administrativas, técnicas y físicas.
Transparencia	Información	Informar a los titulares de los datos personales a través del aviso de privacidad.

Centrado en el usuario	Todos los principios y deberes	Tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa.

De esta manera, el responsable o el encargado que tratan datos personales, pueden y deben adoptar medidas, entre las que deben considerar el modelo de privacidad por diseño, para cumplir con la normatividad sobre protección de datos personales.

3. Referentes internacionales del concepto de privacy by design

3.1 La Resolución de las autoridades de protección de datos y privacidad de 2010

A nivel internacional, el primer referente a destacar es la Resolución sobre Privacidad por Diseño[9], adoptada durante la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que se celebró en Jerusalén, Israel, durante los días 27 a 29 de Octubre de 2010. Se trata, por tanto, de una resolución clave en la materia, ya que fue aprobada de manera unánime por las autoridades de protección de datos y privacidad como un componente esencial para la protección de la privacidad.

En relación con dicha Resolución, es importante destacar algunos aspectos relevantes que permitirán entender su significado y alcance:

- **Carácter internacional:** Lo primero a destacar es el hecho de que se trate de una Resolución aprobada por autoridades de protección de datos y privacidad de varios países alrededor del mundo, lo que demuestra el consenso alcanzado en relación con la misma a nivel internacional.

- **Carácter no vinculante:** no se trata de una resolución vinculante, más allá de ser un instrumento con carácter internacional que permite el desarrollo del concepto de privacidad por diseño en dicho entorno internacional.

- **La resolución no hace referencia específica a la protección de datos personales como tal:** Lo que se deriva del hecho de que sea una Resolución internacional elaborada por autoridades que provienen de diferentes sistemas jurídicos (principalmente derecho anglosajón y derecho continental), que en unos casos protegen la privacidad y en otros la protección de datos personales.

[9] Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners. Disponible, en ingles, en el siguiente vínculo electrónico http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

3.2 Referentes normativos o regulatorios

3.2.1 Unión Europea

En el caso de la normativa vigente a nivel de la Unión Europea, el modelo de privacidad por diseño sí puede encontrarse en algunos artículos de diversas Directivas aplicables en el sector de las comunicaciones electrónicas y, específicamente, se encuentra de manera expresa en la Recomendación 2012/148/UE de la Comisión, de 9 de marzo, relativa a los preparativos para el despliegue inteligente de los sistemas de contador inteligente a la que ya hemos hecho referencia.

Es así que la siguiente tabla tiene por objeto citar la correspondiente norma europea, el artículo correspondiente y el texto relevante:

Norma	Artículo	Materia	Desarrollo
Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad, publicado en el Diario Oficial de la Unión Europea, serie L número 91, de 7 de abril de 1999.	Artículo 3, apartado 3, letra c)	Diseño de equipos radioeléctricos y equipos terminales de telecomunicación	*"[C]ontengan salvaguardias que garanticen la protección de los datos personales y de la intimidad del usuario y del abonado."*
Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector	Artículo 14, apartado 3	Características técnicas y normalización	*"Cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales, de*

Norma	Artículo	Materia	Desarrollo
de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[10], publicada en el Diario Oficial de la Unión Europea, serie L número 201, de 31 de julio de 2002.			*conformidad con la Directiva 1999/5/CE y la Decisión 87/95/CEE del Consejo, de 22 de diciembre de 1986, relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones."*
Recomendación 2012/148/UE de la Comisión, de 9 de marzo, relativa a los preparativos para el despliegue inteligente de los sistemas de contador inteligente, publicada en el Diario Oficial de la Unión Europea, serie L número 73, de 12 de marzo de 2012.	Apartado I, punto 12	Consideraciones relativas a la seguridad y la protección de datos	*"La protección de datos desde el diseño debería aplicarse a los niveles legislativo (por medio de legislación que debe ajustarse a la normativa sobre protección de datos), técnico (incorporando a las normas sobre redes inteligentes requisitos que garanticen que la infraestructura sea plenamente coherente con la normativa sobre protección de datos) y organizativo (en relación con el tratamiento)."*

Nótese que las dos Directivas citadas son posteriores a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos

[10] La citada Directiva ha sido modificada, sucesivamente, por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 , sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, publicada en el Diario Oficial de la Unión Europea, serie L número 105, de 13 de abril de 2006, y por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, publicada en el Diario Oficial de la Unión Europea serie L, número 337, de 18 de diciembre de 2009.

personales y a la libre circulación de estos datos[11], que no contiene tampoco una referencia expresa al modelo de privacidad por diseño.

No obstante, el Supervisor Europeo de Protección de Datos (en adelante, SEPD), ha señalado en su Dictamen acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad[12], que esta Directiva *"contiene disposiciones que, indirectamente, en diferentes situaciones, pueden obligar a aplicar el principio de PdD. En particular, su artículo 17 exige que los responsables del tratamiento apliquen las medidas técnicas y de organización adecuadas para evitar el tratamiento ilícito de los datos. Por lo tanto, la PdD se cubre de manera muy genérica."* (Apartado 30)

También es importante tomar en consideración que la Directiva 2002/58/CE[13] especifica y complementa los principios de la Directiva 95/46/CE en el sector de las comunicaciones electrónicas[14].

En cualquier caso, dichas referencias, tanto las referencias implícitas como las explícitas, salvaguardan la necesaria neutralidad tecnológica. Es decir, la privacidad por diseño y la neutralidad tecnológica son dos principios fundamentales que deben compatibilizarse de manera que el desarrollo de productos y servicios tecnológicos pueda desarrollarse garantizando la necesaria protección de datos personales sin que uno ni otro pueda llegar a suponer una amenaza para el otro.

Además de las referencias a las citadas Directivas y a la Recomendación ya comentada, la Comisión Europea, en enero de 2012, presentó una propuesta de reforma[15] de la Directiva 95/46/CE, con la finalidad de sustituirla mediante un Reglamento general de protección de datos (en adelante, RGPD), directamente

[11] Publicada en el Diario Oficial de la Unión Europea serie L, número 281, de 23 de noviembre de 1995.
[12] Publicado en el Diario Oficial de la Unión Europea serie C, número 280, de 16 de octubre de 2010.
[13] Que derogó a la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, publicada en el Diario Oficial de la Unión Europea, serie L número 24, de 30 de enero de 1998.
[14] Al respecto, el apartado 2, del artículo 1, de la citada Directiva, establece que *"[l]as disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE"*.
[15] Véase la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (Reglamento general de protección de datos), COM(2012) 11 final, de 25 de enero de 2012. Disponible, en español, en el vínculo electrónico http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

aplicable en todos los Estados miembros. Entre las novedades a destacar, la propuesta de RGPD incluye el artículo 23, que regula las obligaciones que tiene el responsable del tratamiento en virtud de la aplicación de los principios de la protección de datos desde el diseño y por defecto.

El considerando 61 de la propuesta de RGPD explica el modelo de privacidad desde el diseño en los siguientes términos:

> *"La protección de los derechos y libertades de los interesados con respecto al tratamiento de datos personales exige la adopción de las oportunas medidas de carácter técnico y organizativo, tanto en el momento del diseño del tratamiento como del tratamiento propiamente dicho, con el fin de garantizar que se cumpla lo dispuesto en el presente Reglamento. Con objeto de garantizar y demostrar el cumplimiento de lo dispuesto en el presente Reglamento, el responsable debe adoptar las políticas internas y aplicar las medidas adecuadas que cumplan especialmente los principios de protección de datos desde el diseño y por defecto."*

En concreto, el artículo 23 establece lo siguiente:

> *"Artículo 23. Protección de datos desde el diseño y por defecto*
>
> *1. Habida cuenta de las técnicas existentes y de los costes asociados a su implementación, el responsable del tratamiento implementará, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, medidas y procedimientos técnicos y organizativos apropiados, de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento y garantice la protección de los derechos del interesado.*
> *2. El responsable del tratamiento implementará mecanismos con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento y, especialmente, que no se recojan ni conserven más allá del mínimo necesario para esos fines, tanto por lo que respecta a la cantidad de los datos como a la duración de su conservación. En concreto, estos mecanismos garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas.*
> *3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar cualesquiera nuevos criterios y requisitos aplicables a las medidas y mecanismos apropiados contemplados en los apartados 1 y 2, en particular en lo que respecta a los requisitos en materia de protección de datos desde el diseño aplicables en el conjunto de los sectores, productos y servicios.*
> *4. La Comisión podrá definir normas técnicas para los requisitos establecidos en los apartados 1 y 2. Dichos actos de ejecución se*

> *adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2."*

Es así que, de aprobarse el RGPD, la Unión Europea contará con un artículo expreso y específico que enuncia el modelo de privacidad desde el diseño y, en la práctica, obliga a los responsables del tratamiento a cumplir con el mismo.

Por último, la propuesta de RGPD se refiere también a este principio al tratar la figura del delegado de protección de datos (en inglés, *Data Protection Officer*, DPO), que es una figura similar al de la persona o departamento de datos personales en México[16], al indicar en el artículo 37, que entre las tareas de aquél están las siguientes:

> *"Artículo 37. Tareas del delegado de protección de datos*
>
> *1. El responsable o el encargado del tratamiento encomendarán al delegado de protección de datos, como mínimo, las siguientes tareas:*
>
> *[…]*
>
> *c) supervisar la implementación y aplicación del presente Reglamento, en particular por lo que hace a los requisitos relativos a la protección de datos desde el diseño, la protección de datos por defecto y la seguridad de los datos, así como a la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos en virtud del presente Reglamento."*

3.2.2. España

Como un ejemplo específico de aplicación de las Directivas europea, cabe señalar que en España, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[17] (en lo sucesivo, LOPD), no hace referencia al modelo de privacidad por diseño, pudiendo encontrarse la explicación de dicha omisión en el hecho de que la Directiva 95/46/CE, la cual transpone al ordenamiento jurídico español, no lo hacía tampoco.

[16] Se trata de la que podríamos denominar "versión europea" del *Chief Privacy Officer* (CPO).

[17] Publicada en el Boletín Oficial del Estado número 298, de 14 de diciembre de 1999. Disponible en el siguiente vínculo electrónico http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

No obstante, es posible considerar que dicho principio sí está implícito en el texto de la norma española, ya que al tratar el principio de calidad de los datos, en el apartado 5, del artículo 4, indica que:

> *"No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados."*

A continuación, en el apartado 6, del citado artículo, también que:

> *"Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados."*

Es decir, la base de datos en la que se traten los datos personales debe estar organizada de manera que, por una parte, sea posible cumplir con el principio de calidad garantizando la minimización del tratamiento y, por otra parte, que su almacenamiento permita el ejercicio del derecho de acceso. En ambos casos, resulta claro que la privacidad por diseño debe tomarse en consideración a la hora de configurar un sistema de información en el que se traten datos personales de manera que permita garantizar la calidad de los datos personales que son objeto de tratamiento en los términos señalados.

Por su parte, el Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre[18], tampoco se refiere expresamente a este principio, si bien cabe entender que sí hace una referencia a la "seguridad por diseño", ya que en relación con productos de software, en su disposición adicional única indica lo siguiente:

> *"Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento."*

[18] Se trata del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el Boletín Oficial del Estado número 17, de 19 de enero de 2008. Disponible en el vínculo electrónico http://www.boe.es/buscar/act.php?id=BOE-A-2008-979

3.3. Otros referentes: guías y otros instrumentos

3.3.1. Guías de autoridades garantes de protección de datos

Diversas autoridades garantes o agencias de protección de datos personales han publicado guías relativas o que se refieren, en su caso, a la privacidad por diseño.

A continuación se hace referencia a estas guías, ya que pueden servir como referentes para el análisis o aplicación del concepto de privacidad por diseño. Es por ello que a continuación, por cada una de las guías que se han identificado, se incluye una tabla en la que se indica la autoridad garante que la ha publicado, la dirección en Internet de la autoridad garante, el vínculo electrónico en el que está disponible la guía y un resumen en relación con la guía.

— Information and Privacy Commissioner of Ontario (Canadá)

Autoridad garante o de protección de datos	**Information and Privacy Commissioner, Ontario, Canada**
Dirección web	http://www.ipc.on.ca
Título de la guía	Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Principles
Vínculo electrónico	http://www.ipc.on.ca/images/Resources/operationalizing-pbd-guide.pdf
Fecha de consulta	9 de febrero de 2014
Resumen	Es una guía para implementar la privacidad por diseño (Privacy by Design, PbD), que pone foco específico en los siete (7) principios fundamentales. En particular, la guía tiene por objeto explicar el significado y alcance de los citados principios fundamentales, que son más amplios que las Fair Information Practices según se indica en la propia guía. El punto de partida, según explica la Dra. Cavoukian, es tomar en consideración la privacidad como un control necesario, vinculándolo así con el derecho a la autodeterminación informativa (*"informational self-determination"*) tal y como fue concebido en Alemania conforme a la Sentencia del Tribunal Constitucional en 1983 sobre el censo. La guía también hace referencia a diversos documentos sobre la privacidad por diseño que han sido publicados a lo largo de varios años de trabajo, en ocasiones en colaboración con compañías internacionales, de manera que permiten ilustrar el desarrollo de este principio desde diferentes perspectivas así como las implicaciones que puede tener para garantizar la protección de datos personales y la privacidad. Por lo tanto, se trata de una guía que trata en profundidad cada uno de los principios de la privacidad por diseño. Además, desde un

	punto de vista organizacional, la privacidad por diseño es un aspecto a tomar en consideración por los diferentes actores que tienen alguna responsabilidad en la materia así como en las políticas sobre privacidad corporativa. Al respecto, la guía incluye, por cada principio, una tabla que presenta acciones a tomar en consideración y la asignación de responsabilidades en el marco del organigrama de una organización así como a diferentes actores que puedan estar involucrados en la materia, tales como reguladores o desarrolladores de productos de TI. Por último, la guía incluye varios anexos que tienen por objeto ofrecer ejemplos prácticos de la privacidad por diseño y sus principios aplicados a diferentes áreas de actividad, tales como los dispositivos móviles y las comunicaciones, las RFID y los sensores o el big data. En total, se trata de nueve (9) áreas clave de aplicación de los principios de privacidad por diseño. Además, por cada una de estas áreas, incluye una lista de documentos donde se puede encontrar más información sobre la materia.

— Information Commisioner´s Office (Reino Unido)

Autoridad garante o de protección de datos	**Information Commissioner´s Office (Reino Unido)**
Dirección web	http://ico.org.uk
Título de la guía	Privacy by Design Report
Vínculo electrónico	http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PRIVACY_BY_DESIGN_REPORT_V2.ashx
Fecha de consulta	9 de febrero de 2014
Resumen	En este informe de la autoridad británica de protección de datos personales parte del hecho de que la privacidad por diseño no ha sido debidamente atendida durante los últimos años y se proponen recomendaciones que pueden ser adoptadas para asegurar la protección de la privacidad. Se trata de una guía dirigida tanto al sector público como al privado de manera que adopten medidas para garantizar la protección de datos personales a través de la privacidad por diseño. En particular, con esta guía la autoridad garante del Reino Unido busca identificar vacíos o asuntos clave con la finalidad de que las recomendaciones que incluyen sean tomadas en consideración por los destinatarios con la finalidad de garantizar el derecho a la protección de datos personales y la privacidad. Al respecto, la guía incluye varias tablas en las que se tratan diversas cuestiones y en las que se incluyen las correspondientes recomendaciones para impulsar la privacidad por diseño en cada caso. Así, por ejemplo, se incluyen tablas relativas a las barreras u obstáculos a la privacidad por diseño, la seguridad por diseño. En concreto, la guía se divide en cuatro partes, relativas a: 1) la privacidad por diseño como un reto; 2) las barreras a la privacidad por diseño; 3) las acciones a tomar para desarrollar la privacidad por

	diseño, y 4) recomendaciones para desarrollar la privacidad por diseño. Por lo tanto es una guía que trata las cuestiones que se plantean en torno al concepto de privacidad por diseño, su desarrollo y la necesidad de adoptar medidas concretas para impulsar dicha aproximación de manera que ello permita garantizar la protección de datos personales y la privacidad.

— Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Alemania)

Autoridad garante o de protección de datos	***Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit***
Dirección web	*http://www.bfdi.bund.de*
Título de la guía	*Privacy by design*
Vínculo electrónico	*http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/0610EUPrivacyByDesign.pdf?__blob=publicationFile*
Fecha de consulta	*28 de febrero de 2014*
Resumen	*El documento de la autoridad garante alemana introduce el concepto de privacidad por diseño haciendo referencia que, a la vista de la Directiva 95/46/CE, no se trata de un concepto completamente nuevo, sino que el considerando 46 de dicha norma explica la necesidad de adoptar medidas técnicas y apropiadas para garantizar, específicamente, la seguridad y, con carácter general, la protección de los datos personales.* *El citado considerando 46 de la Directiva 95/46/CE indica que "la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado".* *En particular, el documento explica que la privacidad por diseño va más allá de mantener la seguridad, ya que significa que los sistemas de información deberían ser diseñados y desarrollados de manera que eviten o minimicen la cantidad de datos personales tratados. A tal fin, el documento presenta varios ejemplos para demostrar cómo la privacidad por diseño puede ayudar a garantizar la protección de datos personales. Dichos ejemplos se refieren, entre otros, a la tarjeta sanitaria electrónica y la cédula de identidad electrónica.*

— Office of the Australian Information Commissioner (Australia)

Autoridad garante o de protección de datos	**Office of the Australian Information Commissioner**
Dirección web	http://www.oaic.gov.au

Título de la guía	Mobile privacy: a better practice guide for mobile app developers
Vínculo electrónico	http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-for-mobile-app-developers/privacy-by-design
Fecha de consulta	9 de febrero de 2014
Resumen	Se trata de una guía[19] dirigida específicamente al entorno de desarrolladores de aplicaciones móviles (*"apps"*), tanto del sector público como del privado, con la finalidad de concientizarles sobre la necesidad de garantizar la protección de datos personales y la privacidad a través de la privacidad por diseño. Resulta importante señalar que la guía está dirigida a los desarrolladores de aplicaciones móviles con independencia de que traten o no datos personales, de manera que se quiere así involucrar a todos los actores económicos ya que desempeñan un papel importante a la hora de ayudar a garantizar la protección de datos personales y la privacidad. Es así que se pone de manifiesto la necesidad de que los desarrolladores de aplicaciones sigan el enfoque de la privacidad por diseño de manera que apliquen prácticas de protección de la privacidad (en inglés, *"privacy-enhancing practices"*) a lo largo del ciclo de vida de los datos personales que son objeto de tratamiento. Además, la autoridad garante australiana ofrece una lista de verificación[20] (*"checklist"*) para desarrolladores de aplicaciones móviles, con la finalidad de que puedan hacer uso de la misma para comprobar el grado de cumplimiento en cuanto a las prácticas en protección de datos personales que sigan.

— Federal Trade Commission (Estados Unidos)

Autoridad garante o de protección de datos	**Federal Trade Commission**
Dirección web	http://www.ftc.gov
Título de la guía	Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers
Vínculo electrónico	http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
Fecha de consulta	9 de febrero de 2014
Resumen	El informe de la Comisión Federal de Comercio (en inglés, *Federal Trade Commission*, FTC) pretende ser una llamada de atención sobre la necesidad de implementar buenas prácticas para proteger la privacidad de los consumidores, de manera que está dirigido tanto a empresas, ya sean responsables o encargados, como a desarrolladores de políticas públicas. Se trata de un informe que trata diversas cuestiones sobre la protección de la privacidad, entre las que se incluye la privacidad por diseño, a la que dedica un

[19] Una versión completa de la guía puede verse, en inglés, en el siguiente vínculo electrónico http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/better-practice-guide-for-mobile-developers.pdf

[20] Disponible, en inglés, en el vínculo electrónico http://www.oaic.gov.au/images/documents/privacy/privacy-guides/Better_practice_guide_for_mobile_developers__Appendix_A.pdf

	apartado específico. Con respecto a la privacidad por diseño, el informe recomienda específicamente que las organizaciones promuevan la protección de la privacidad de los consumidores a lo largo de toda la organización y en cada etapa del desarrollo de sus productos y servicios. El informe señala que ya hay empresas que han incluido medidas sustantivas y procedimentales para la protección de la privacidad en sus prácticas empresariales, si bien llama la atención sobre la necesidad de que la industria implemente la privacidad por diseño de manera más sistemática. Cabe destacar el hecho de que el informe, por lo que se refiere a la privacidad por diseño, haga referencia a que si bien no cambia los principios fundamentales propuestos, responde a comentarios recibidos que sugieren la incorporación de principios adicionales, tales como las medidas de seguridad, límites razonables a la obtención de datos personales, prácticas sobre retención de datos personales o sobre la calidad (exactitud) de los mismos. Por último, el informe concluye este apartado específico sobre la privacidad por diseño con la recomendación, como principio a seguir, de que las organizaciones mantengan procedimientos comprehensivos de gestión de datos personales a lo largo del ciclo de vida de sus productos y servicios, lo que obviamente supone aplicar medidas sustantivas y procedimentales en esta materia.
Autoridad garante o de protección de datos	**Federal Trade Commission**
Dirección web	http://www.ftc.gov
Título de la guía	Marketing your Mobile App, Get it right from the start.
Vínculo electrónico	http://business.ftc.gov/sites/default/files/pdf/bus81-marketing-your-mobile-app.pdf
Fecha de consulta	9 de febrero de 2014
Resumen	En esta guía dirigida específicamente a desarrolladores de aplicaciones (*"apps"*) que quieren hacer marketing de las mismas, la Comisión Federal de Comercio (en inglés, *Federal Trade Commission*, FTC) ofrece recomendaciones para cumplir con estándares de publicidad lícita (*"truth-in-advertising"*) y principios básicos de privacidad. En concreto, en materia de privacidad por diseño, la FTC explica brevemente su significado, recomendando su aplicación y cumplimiento de manera que las aplicaciones ofrecidas garanticen la privacidad de los usuarios. Es así que al desarrollar aplicaciones que observan la privacidad por diseño, se cumple con los principios de la protección de la privacidad de los usuarios, garantizando también su expectativa de privacidad.

— Information Commissioner (Eslovenia)

Autoridad garante o de protección de datos	**Information Commissioner (Informacijski Pooblačěenec)**
Dirección web	https://www.ip-rs.si
Título de la guía	Guidelines for developing information solutions
Vínculo electrónico	https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_razvoj_informacijski_resitev_ENG.pdf
Fecha de consulta	9 de febrero de 2014
Resumen	Con esta guía la autoridad garante eslovaca ofrece recomendaciones a tomar en consideración en el desarrollo de productos y servicios tecnológicos con la finalidad de garantizar la protección de datos personales. La guía está dirigida tanto a responsables como encargados del tratamiento, proporcionándoles consejos prácticos. Por lo que se refiere a la privacidad por diseño en particular, la autoridad garante la introduce como una ventaja competitiva, haciendo además referencia a que será incluido en el futuro Reglamento General de Protección de Datos. También hace referencia a que la evaluación de impacto de privacidad (en inglés, *Privacy Impact Assessment*, PIA), es un elemento esencial para hacer efectiva la privacidad por diseño. Además de hacer referencia a los siete principios fundamentales de la privacidad por diseño, la guía también hace referencia a la necesidad de garantizar la seguridad de los datos personales a lo largo del ciclo de vida de su tratamiento. En cuanto a los principios, la guía incluye también referencias a otros principios tales como la minimización, la proporcionalidad, así como las medidas de seguridad y el derecho de acceso.

3.3.2 Otros instrumentos

Entre otros instrumentos, es posible hacer referencia a diversos Dictámenes del Supervisor Europeo de Protección de Datos (en adelante, SEPD).

La siguiente tabla incluye los Dictámenes del SEPD en los que se hace referencia al modelo de privacidad por diseño. Es así que la tabla incluye la referencia al Dictamen correspondiente, la referencia al modelo de privacidad por diseño y el vínculo electrónico donde se puede consultar el correspondiente Dictamen:

Título del dictamen	Referencia al modelo de privacidad por diseño	Vínculo electrónico
Dictamen del Supervisor Europeo de	La necesidad de	https://secure.edps.europa.eu/

Título del dictamen	Referencia al modelo de privacidad por diseño	Vínculo electrónico
Protección de Datos relativo a la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «La identificación por radiofrecuencia (RFID) en Europa: Pasos hacia un marco político», documento COM(2007) 96, publicado en el Diario Oficial de la Unión Europea serie C, número 101, de 23 de abril de 2008.	"intimidad mediante el diseño", apartados 51 a 55.	EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social «Hacia una estrategia europea en materia de e-Justicia (Justicia en línea)», publicado en el Diario Oficial de la Unión Europea serie C, número 128, de 6 de junio de 2009.	Apartado 24.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-19_eJustice_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión relativa a un Plan de acción para el despliegue de sistemas de transporte inteligentes en Europa y a la propuesta que lo acompaña de Directiva del Parlamento Europeo y del Consejo por la que se establece el marco para el despliegue de los sistemas de transporte inteligentes en el sector del transporte por carretera y para sus interfaces con otros modos de transporte, publicado en el Diario Oficial de la Unión Europea serie C, número 47, de 25 de febrero de 2010.	Apartados 28 a 30.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, publicado en el Diario Oficial de la Unión Europea serie C, número 280, de 16 de octubre de 2010.	Apartados 16 a 57.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del	Apartados 32 a 34.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultat

Título del dictamen	Referencia al modelo de privacidad por diseño	Vínculo electrónico
Parlamento Europeo y del Consejo sobre residuos de aparatos eléctricos y electrónicos (RAEE), publicado en el Diario Oficial de la Unión Europea serie C, número 280, de 16 de octubre de 2010.		ion/Opinions/2010/10-04-14_Opinion_WEEE_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Consejo y al Parlamento Europeo — «Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia», publicado en el Diario Oficial de la Unión Europea serie C, número 355, de 29 de diciembre de 2010.	Apartados 36 y 37.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-09-30_Freedom_security_Justice_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta modificada de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (CE) nº (…/…) (por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida), publicado en el Diario Oficial de la Unión Europea serie C, número 101, de 1 de abril de 2011.	Apartado 31.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-12-15_EURODAC_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre un proyecto de investigación financiado por la Unión Europea dentro del Séptimo Programa Marco (7PM) para la Investigación y Desarrollo Tecnológico – Turbine (Identidades Biométricas Revocables y de Confianza)[21].	Apartados 5, 16, 66 y 67.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf
Dictamen del Supervisor Europeo de Protección de Datos relativo a la	Apartados 48 y 49.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySit

[21] El título original del Dictamen, en inglés, es Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs).

Título del dictamen	Referencia al modelo de privacidad por diseño	Vínculo electrónico
Decisión 2011/141/UE de la Comisión que modifica la Decisión 2007/76/CE de la Comisión sobre el Sistema de Cooperación para la Protección de los Consumidores (CPCS) y sobre la Recomendación 2011/136/UE de la Comisión sobre las directrices para la aplicación de las normas de protección de datos en el CPCS, publicado en el Diario Oficial de la Unión Europea serie C, número 217, de 23 de julio de 2011.		e/shared/Documents/Consultation/Opinions/2011/11-05-05_CPCS_consul_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre migración, publicado en el Diario Oficial de la Unión Europea serie C, número 34, de 8 de febrero de 2012.	Apartados 16 y 18.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-07-07_Migration_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre las propuestas legislativas relativas a la resolución alternativa y en línea de litigios en materia de consumo, publicado en el Diario Oficial de la Unión Europea serie C, número 136, de 11 de mayo de 2012.	Apartado 21.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-01-11_Online_Dispute_Resolution_ES.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre la represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia[22].	Apartados 33 y 34.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-29_European_Cybercrime_Center_EN.pdf
Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión sobre el Plan de acción sobre la salud electrónica 2012-2020 – atención sanitaria innovadora para el siglo XXI[23].	Apartados 19 a 23.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-03-27_eHealth_Action_EN.pdf

[22] El título original del Dictamen, en inglés, es Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre.

[23] El título original del Dictamen, en inglés, es Opinion of the European Data Protection Supervisor on the Communication from the Commission on ´eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century´.

Título del dictamen	Referencia al modelo de privacidad por diseño	Vínculo electrónico
Dictamen del Supervisor Europeo de Protección de Datos sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas en relación con el mercado único europeo de las comunicaciones electrónicas y para crear un continente conectado, y se modifican las Directivas 2002/20/CE, 2002/21/CE y 2002/22/CE y los Reglamentos (CE) nº 1211/2009 y (UE) nº 531/2012.[24]	Apartados 38 a 42.	https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-11-14_Single_Market_Electronic_Communications_EN.pdf

A lo largo de sus diversos y sucesivos Dictámenes, el Supervisor Europeo de Protección de Datos (SEPD), ha ido desarrollando, en su ámbito de actuación, el concepto de privacidad por diseño en la Unión Europea. Es decir, sus Dictámenes, emitidos en virtud de su función de consulta, sirven para desarrollar políticas públicas que, en el presente caso, se centran en la privacidad por diseño.

De entre los diferentes Dictámenes que ha emitido en la materia hasta la fecha, cabe destacar su Dictamen acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, publicado en el Diario Oficial de la Unión Europea serie C, número 280, de 16 de octubre de 2010.

En dicho Dictamen, el SEPD incide en el hecho de que las implicaciones que en la práctica tienen las tecnologías de la información y la comunicación (TIC), prestando especial atención a las capacidades enormes que estas tienen en todos los aspectos y ámbitos de nuestra vida actual. Es así que el SEPD, reconociendo los beneficios de las TIC, indica que *"la UE debería hacer todos los esfuerzos posibles para impulsar su desarrollo y para que el acceso a ellas sea generalizado"*, si bien no puede tratarse de un desarrollo a cualquier precio. Es así que *"las personas han de ser capaces de hacer uso de la capacidad de las TIC de mantener su información segura y controlar su utilización, así como confiar en que en el espacio digital se respetarán su privacidad y sus derechos de protección"*.

[24] El título original del Dictamen, en inglés, es Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) Nº 1211/2009 and (EU) Nº 531/2012.

En concreto, el Dictamen trata la cuestión relativa a cumplir con el modelo de privacidad por diseño de manera que el desarrollo tecnológico se haga conforme a los principios de la protección de datos personales, lo que permitirá garantizar el derecho fundamental de los titulares de los datos personales. Se trata, por tanto, de desarrollar tecnología que, desde el inicio, cumpla con los principios de la protección de datos personales lo que se consigue a través de la aplicación del modelo de privacidad por diseño.

El Dictamen se refiere también a las recomendaciones del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE[25], en su Dictamen 2/2008 sobre la revisión de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (Directiva sobre privacidad)[26], de manera que este principio *"debería ser vinculante para los diseñadores y productores de tecnología y para los responsables del tratamiento que tengan que decidir sobre la adquisición y el uso de las TIC, que deberían estar obligados a tener en cuenta la protección tecnológica de los datos ya desde la fase de planificación de los procedimientos y sistemas tecnológicos de información"*[27].

Minimizar el tratamiento de los datos personales, además de garantizar el resto de principios y deberes de la protección de datos personales, a través de la implementación de mejores tecnologías, es lo que permite tanto a los responsables como a los encargados del tratamiento, garantizar el derecho fundamental a la protección de datos personales.

En definitiva, la aplicación del modelo de privacidad por diseño trata de asegurar, desde la fase inicial de desarrollo de un sistema de información o planteamiento de un modelo de negocio y durante todo el ciclo de vida, la protección de datos personales a través de la aplicación de los principios y deberes exigibles.

De esta manera se trata de disminuir a su grado mínimo el costo de la aplicación de dicha normatividad así como el riesgo que conlleva todo tratamiento de datos personales, que en caso de verificación de un incumplimiento puede dar lugar a

[25] El referido Grupo de Trabajo, establecido en virtud del artículo 29 de la Directiva 95/46/CE, tiene carácter consultivo e independiente. Para más información sobre dicho Grupo, puede verse el siguiente vínculo electrónico http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[26] WP 150, emitido el 15 de mayo de 2008 y disponible en el siguiente vínculo electrónico http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_es.pdf

[27] Apartado 40 del Dictamen del Supervisor Europeo de Protección de Datos, ya citado.

sanciones económicas, además de la pérdida de confianza de las partes interesadas entre las que se encuentran los clientes, que son titulares de los datos personales objeto del tratamiento.

4. Análisis práctico en la LFPDPPP y su Reglamento: principios y deberes

4.1 La LFPDPPP

Por lo que se refiere a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[28] (en adelante, LFPDPPP), esta no hace referencia expresa en su articulado al modelo de privacidad por diseño.

Es así que si revisamos el texto de la versión final del Dictamen de la LFPDPPP[29], no se encuentra ninguna referencia expresa a este principio. Ello a pesar de que la Comisión de Gobernación:

> *"destaca la importancia de la presente Ley en potencia, toda vez que con un ordenamiento jurídico de esta naturaleza, nuestro país se haría más competitivo en el ámbito mundial, ubicándose en posición de privilegiado en el aspecto económico, ya que al contar con una ley específica en la materia, no sólo se permitirá al gobernado ejercer eficazmente un nuevo derecho fundamental, sino que también traerá consigo que nuestro país, pueda ampliar su relación comercial con bloques económicos de la importancia de la Unión Europea, toda vez que nos encontraremos en posibilidades de garantizar conforme a los estándares internacionales, un nivel de protección de datos personales adecuado al prever principios y derechos de protección y una autoridad independiente que los garantice."*

Ahora bien, el dictamen de la Comisión de Gobernación y la promulgación de la LFPDPPP son anteriores a la Resolución sobre Privacidad por Diseño aprobada por las autoridades de protección de datos y privacidad, aprobada también en 2010 y anteriormente mencionada.

Como hemos indicado, la LFPDPPP tampoco hace referencias expresas al modelo de privacidad por diseño, si bien es posible identificar algunas referencias indirectas, que son las que se indican en la siguiente tabla:

[28] Publicada en el Diario Oficial de la Federación de 5 de julio de 2010.

[29] Dictamen con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de la Comisión de Gobernación, publicado en el siguiente vínculo electrónico http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf

LFPDPPP	Desarrollo
Art. 14	*"El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable."*
Art. 22	*"Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos."*

Estas dos referencias son relevantes ya que, por un lado, el responsable debe adoptar las medidas necesarias para garantizar el cumplimiento de los principios de la protección de datos, lo que, entre otros aspectos, supone considerar la protección de datos desde el momento mismo de diseño de la base de datos o el tratamiento que se realice. Y, por otro lado, resguardar los datos personales de manera que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) sin dilación, implica también que se deban adoptar medidas en cuanto al diseño de la base de datos o sistema de información en el que se traten con la finalidad de garantizar la atención de los mismos y, por tanto, el derecho fundamental a la protección de datos personales.

Sin perjuicio de lo anterior, es necesario prestar atención a la reciente reforma constitucional en materia de transparencia[30], en virtud de la que se otorga autonomía y más atribuciones al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) que tiene importantes implicaciones también en materia de protección de datos personales[31] ya que el Congreso de la Unión reformará la LFPDPPP[32].

Dicha reforma puede ser una oportunidad para incluir algunos aspectos que, en la medida de lo posible, mejoren la LFPDPPP, como por ejemplo incluir referencias expresas a este modelo de privacidad por diseño.

[30] Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el Diario Oficial de la Federación de 7 de febrero de 2014 y disponible en el siguiente vínculo electrónico http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014

[31] Al respecto, véase la nota de prensa (referencia IFAI-OA/001/14) publicada por el IFAI con fecha 14 de febrero de 2014 y disponible en el siguiente vínculo electrónico http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-001-14.pdf

[32] Véase el artículo transitorio segundo del citado Decreto de reforma constitucional en materia de transparencia.

4.2 El Reglamento

El Reglamento de la LFPDPPP tampoco hace referencia expresa, como tal, al modelo de privacidad por diseño, si bien los artículos 47 y 48, que desarrollan el principio de responsabilidad, podrían considerarse como una manifestación de aquél, ya que exigen que el responsable adopte medidas para garantizar la protección de datos personales.

Es así que en la siguiente tabla se incluyen las referencias relevantes de cada uno de estos artículos:

Reglamento de la LFPDPPP	Desarrollo
Art. 47. *Principio de responsabilidad*	*"En términos de los artículos 6 y 14 de la Ley, el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.* *Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines."*
Art. 48. *Medidas para el principio de responsabilidad*	*"En términos del artículo 14 de la Ley, el responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.* *Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:* *I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;* *II. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;* *III. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;*

Reglamento de la LFPDPPP	Desarrollo
	IV. Destinar recursos para la instrumentación de los programas y políticas de privacidad; *V. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;* *VI. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;* *VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;* *VIII. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;* *IX. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento, o* *X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento."*

En el caso del artículo 47 del Reglamento, el hecho de que el responsable pueda valerse de estándares, mejores prácticas internacionales o, incluso, cualquier otro mecanismo que determine adecuado para tales fines, permite afirmar que se trata de una clara referencia al modelo de privacidad por diseño.

Es decir, el responsable puede recurrir a este modelo de privacidad por diseño para cumplir con el principio de responsabilidad, de manera que el cumplimiento de la normatividad sobre protección de datos personales, los principios, deberes y derechos ARCO, se consigan a través del mismo.

Asimismo, entre las medidas a que hace referencia el artículo 48 del Reglamento de la LFPDPPP, cabe destacar la prevista en la fracción V, que si bien consiste en realizar una evaluación del impacto de privacidad (en inglés, PIA), está estrechamente relacionada con la privacidad por diseño ya que implica considerar desde el diseño de productos, servicios o modelos de negocio, la aplicación de

controles que permitan minimizar el riesgo que implica todo tratamiento de datos personales.

4.3 Otra normatividad a considerar

Además de la LFPDPPP y su Reglamento, es posible hacer referencia a otra normatividad relevante que se debe tomar en consideración en relación con el modelo de privacidad por diseño. Es por ello que a continuación se efectúan las consideraciones oportunas en la materia, comenzando por los Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante y siguiendo con normatividad sectorial específica en el ámbito de las telecomunicaciones.

4.3.1 Parámetros de autorregulación vinculante

Los Parámetros de Autorregulación en materia de Protección de Datos Personales[33], que en desarrollo de lo previsto en la LFPDPPP y su Reglamento, tienen por objeto *"establecer reglas, criterios y procedimientos para el correcto desarrollo e implementación de los esquemas de autorregulación vinculante en materia de protección de datos personales"* (parámetro primero), prevén que en cuanto a los esquemas de autorregulación vinculante que *"podrán incluir principios, normas y procedimientos para adecuar y armonizar las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, a la realidad de sectores específicos, y abordar problemáticas o situaciones particulares que no fueron previstas por la norma general, a fin de hacer eficiente la protección de datos personales en las actividades que se autorregulen.*

Asimismo, la autorregulación vinculante permitirá elevar los estándares de protección de datos personales, a través de la adopción de las mejores prácticas en la materia, tanto nacionales como internacionales" (parámetro sexto).

Al establecer que la autorregulación vinculante permitirá elevar los estándares de protección de datos personales tomando en consideración *"las mejores prácticas en la materia, tanto nacionales como internacionales"*, dicha referencia incluye, también, el modelo de privacidad por y desde el diseño.

[33] Publicados en el Diario Oficial de la Federación el 29 de mayo de 2014, disponibles en http://dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014 y que abrogan a los Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que habían sido publicados en el Diario Oficial de la Federación el 17 de enero de 2013.

Es así que tanto el responsable como el encargado del tratamiento al adoptar un esquema de autorregulación vinculante podrían incluir medidas específicas en materia de privacidad por diseño.

Por último, los esquemas de autorregulación vinculante, tal y como señala el parámetro noveno, pueden consistir en *"reglas emitidas con objeto de adaptar la normativa aplicable en materia de protección de datos personales a la realidad y actividades de un sector en particular"* (fracción I), *"esquemas de autorregulación vinculante evaluados y validados por el Instituto"* (fracción II) y *"esquemas de autorregulación vinculante certificados por un organismo de certificación en materia de protección de datos personales"* (fracción III).

4.3.2 Ley Federal de Telecomunicaciones y Radiodifusión

La LFPDPPP y su Reglamento constituyen la normatividad general en materia de protección de datos personales en el sector privado en México y se aplican sin perjuicio de la normatividad específica que pueda resultar aplicable.

Esto es lo que ocurre en el sector de las telecomunicaciones, en el que hay que tomar en consideración la Ley Federal de Telecomunicaciones y Radiodifusión[34] (en adelante, LFTyR), que es la normatividad específica para dicho sector.

En particular, resulta relevante la fracción II, del artículo 191 de la LFTyR, que reconoce el derecho *"a la protección de los datos personales en términos de las leyes aplicables"*, debiendo ponerlo en conexión tanto con la Ley Federal de Protección al Consumidor[35], que es otra norma específica que se refiere a la protección de datos personales de los consumidores, así como con la normatividad general en protección de datos personales, ya mencionada.

Y también, la fracción III, del artículo 145 de la LFTyR, que se refiere a que los concesionarios y autorizados que presten servicios de acceso a Internet, en virtud de los Lineamientos de carácter general que expida el Instituto Federal de Telecomunicaciones, tendrán que *"preservar la privacidad de los usuarios y la seguridad de la red."*

[34] Esta Ley fue publicada en el Diario Oficial de la Federación el 14 de julio de 2014 y puede verse en la dirección de Internet http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014 Hay que tomar en consideración que dicha Ley abroga, en virtud de su artículo transitorio segundo, la Ley Federal de Telecomunicaciones, que estaba vigente hasta el momento.

[35] Publicada en el Diario Oficial de la Federación de 24 de diciembre de 1992 y que puede verse en la dirección de Internet http://www.diputados.gob.mx/LeyesBiblio/pdf/113_040614.pdf

Estas dos referencias son importantes ya que los concesionarios y autorizados, en virtud de la normatividad sobre protección de datos personales y privacidad, tanto general como específica, tendrán que adoptar medidas para garantizar el derecho fundamental a la protección de datos personales.

Al respecto, la referencia que hace la fracción II, del artículo 191 de la LFTyR a la protección de datos personales en términos de las leyes aplicables, implica que deban adoptarse medidas para cumplir con el principio de responsabilidad (artículos 14 de la LFPDPPP y 48 del Reglamento de la LFPDPPP), además de otras normas que sean aplicables, y ello pasa por adoptar medidas desde el diseño de los sistemas de tratamiento de los datos personales, las bases de datos personales y los productos o servicios que ofrezcan a los usuarios.

Estas medidas deben buscar, incluso cuando no se menciona expresamente el modelo de privacidad por y desde el diseño, garantizar la protección de datos personales y privacidad de los usuarios de servicios de telecomunicaciones, protegiendo así su derecho fundamental.

En definitiva, a pesar de que la LFTyR, al igual que ocurría con la Ley a la que abroga, tampoco hace mención expresa del modelo de privacidad por diseño, las referencias a la protección de los datos personales en términos de las leyes aplicables y a preservar la privacidad de los usuarios pueden entenderse como una referencia implícita al modelo de privacidad por diseño, extendiéndose dichas medidas tanto al responsable como, en su caso, al encargado del tratamiento.

5. Ann Cavoukian: creadora del concepto privacy by design

5.1 Introducción

Una parte importante de este trabajo de investigación fue lograr una entrevista con la precursora del PbD, la Dra. Ann Cavoukian, quien fuera Comisionada de la Oficina de privacidad e información de Ontario, Canadá. Para llevar a cabo esta fase, se elaboraron las pautas del cuestionario o preguntas de la entrevista, mismas que obtuvieron la no objeción por parte de CANIETI y la Dirección de Economía Digital de la Secretaría de Economía.

En este apartado se expone una semblanza de la entrevistada, la pauta de cuestionario, los antecedentes de consultas entre Consultor y Beneficiario y, desde luego, el resultado de la entrevista.

5.2 Semblanza de la Dra. Ann Cavoukian

Ann Cavoukian

Nació en 1952 en El Cairo, Egipto. Hija de padres armenios emigró a Toronto. Canadá en 1958, lugar donde estudió un BA en la Universidad de York. Cuenta con maestría y doctorado en sicología por la Universidad de Toronto y se ha especializado en criminología y derecho.

En la década de los ochentas dirigió la Oficina de Servicios de Investigación de la Fiscalía General de la Provincia de Ontario y en 1987 se incorporó a la Oficina del

Comisionado de Información y Privacidad durante su etapa de arranque, fungiendo como su primer Director de Cumplimiento.

En 1990, fue nombrada Comisionada Asistente y desde 1997 a 2014 fungió como Comisionada de la Oficina de privacidad e información de Ontario, Canadá.

Su destacado desempeño en la supervisión, en los ámbitos del derecho a la información y privacidad, en la provincia más poblada de Canadá, motivó que el término de su encargo fuese ha ampliado a 2014 con motivo de tres reelecciones, lo que se considera un hecho sin precedentes en aquel país.

La Dra. Cavoukian es reconocida como una de las principales expertas de privacidad en el mundo, por lo que empresas importantes de Estados Unidos, Canadá y Europa le solicitan orientación sobre herramientas y política en materia de protección de datos personales.

En 2003, una publicación líder de privacidad anunció a la Dra. Cavoukian como *The Privacy Manager del Año.* Además, en 2005, el Foro Europeo de Biométrica (EBF) anunció la creación del Consejo Asesor Internacional Biometric y nombró a la Dra. Ann Cavoukian como miembro del Consejo.

En 2005, fue galardonada con el *Premio a la Innovación de Privacidad* a la mayor reunión de profesionales de la privacidad en poder de la Asociación Internacional de Profesionales de la Privacidad. La Comisionada Cavoukian y su Oficina fueron reconocidas por el desarrollo innovador de los “avisos de privacidad cortos”.

En noviembre de 2006, la Dra. Cavoukian fue honrada por la Asociación de Abogados de Ontario por "*sus contribuciones sobresalientes a la protección de los derechos de privacidad en Ontario, incluido su papel de liderazgo en la participación tanto del sector público como privado, y su éxito en la promoción de la comprensión y el respeto por el acceso a la información y la privacidad de los derechos*".

En 2011 fue reconocida como una de las Mujeres más influyentes de Canadá, distinción que le siguió a su reconocimiento en 2007 por parte de las Top 100 mujeres más poderosas de Canadá. Ha obtenido igualmente el prestigioso *Premio Kristian Beckman* por su trabajo pionero sobre *Privacy by Design* y la protección de la privacidad en entornos internacionales modernos.

Es autora de los libros "Who Knows: Safeguarding Your Privacy in a Networked World" (1997), escrito con Don Tapscott, y "The Privacy Payoff: How Successful Businesses Build Customer Trust" (2002), en coautoría con Tyler Hamilton.

Ann Cavoukian introdujo el concepto que se conoce por PbD (Privacy by Design – Privacidad desde el Diseño), que busca una relación win-win (ganar-ganar) en los nuevos proyectos que sean susceptibles de incorporar datos personales. Se trata de un concepto valioso para la economía digital que está inmersa en la gran cantidad de información digitalizada, por lo que los negocios tienen una vocación de basarse en los datos de las personas en el Big Data, las técnicas analíticas, prospección de mercados, marketing, etc., pero todo en un justo equilibrio entre los beneficios de las tendencias innovadoras y los riesgos relacionados con la privacidad.

Como se apuntó en el primer entregable, la PbD fue creada por la Dra. Ann Cavoukian y reconocida como estándar global de privacidad en octubre de 2010 a través de la Resolución sobre Privacidad por Diseño[36], adoptada durante la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, tiene por objeto servir como aproximación de manera que los nuevos modelos o prácticas de negocio, las especificaciones tecnológicas y las infraestructuras físicas incluyan principios de privacidad de manera que respeten el derecho fundamental a la protección de datos personales.

[36] Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners. Disponible, en inglés, en el siguiente vínculo electrónico http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

5.3 Diseño de los Contenidos de la Entrevista

Para el diseño de las preguntas (en los idiomas inglés y español) para la entrevista a la Dra. Ann Cavoukian, se tomaron como pauta conceptos relacionados con el análisis de los principios del PbD; beneficios de la implementación en las empresas; papel o rol de las Tecnologías de Información; facilidad de implementación en las empresas; casos de éxito desarrollados; retos de la implementación del modelo.

El eje central del cuestionario fue tener elementos emanados de la propia autora del concepto de PbD que sirvan como referentes a las MIPYMES del sector de las Tecnologías de la Información (TI) de México para que lo puedan aprovechar o replicar su caso y se fomente el cumplimiento de la normatividad sobre protección de datos personales. La pauta de entrevista es la siguiente:

INTERVIEW WITH DR. (PH.D.) ANN CAVOUKIAN, ONTARIO INFORMATION AND PRIVACY COMMISSIONER, ON THE CONCEPT OF PRIVACY BY DESIGN	**ENTREVISTA CON LA DRA. ANN CAVOUKIAN, COMISIONADA DE INFORMACIÓN Y PRIVACIDAD DE ONTARIO (CANADÁ), SOBRE LA PRIVACIDAD DESDE EL DISEÑO**
1.– What is the meaning of privacy and why it matters? What is your opinion about current issues around the world where privacy is involved? Do you think that privacy is in peril somehow or this is a moment to encourage it?	1.– ¿Cuál es el significado de privacidad y por qué es relevante? ¿Cuál es su opinión sobre los asuntos actuales alrededor del mundo en los que la privacidad está involucrada? ¿Considera que la privacidad está en peligro de alguna manera o que éste es un momento para impulsarla?
2.– When and why did you create privacy by design? What is the meaning and scope of privacy by design?	2.– ¿Cuándo y por qué creó usted la privacidad por diseño? ¿Cuál es el significado y alcance de la privacidad por diseño?
3.– Privacy by design as a privacy and data protection principle, how could you explain it for engineers and lawyers at the same time? “Privacy into the code” should be a meeting point for them?	3.– Privacidad por diseño como un modelo de privacidad y protección de datos, ¿cómo puede explicarlo a ingenieros y abogados al mismo tiempo? ¿Debería ser la “privacidad en el código” un punto de encuentro para ellos?
4.– Do you think that “privacy into the code”	4.– ¿Considera que la “privacidad embebida en

INTERVIEW WITH DR. (PH.D.) ANN CAVOUKIAN, ONTARIO INFORMATION AND PRIVACY COMMISSIONER, ON THE CONCEPT OF PRIVACY BY DESIGN	ENTREVISTA CON LA DRA. ANN CAVOUKIAN, COMISIONADA DE INFORMACIÓN Y PRIVACIDAD DE ONTARIO (CANADÁ), SOBRE LA PRIVACIDAD DESDE EL DISEÑO
could be a starting point also for regulators and legislators?	el código" podría ser un punto de partida también para autoridades reguladoras y legisladores?
5.– Is privacy by design both for the private and public sectors? And is its also both for data controllers and data processors?	5.– ¿Es la privacidad por diseño tanto para el sector privado como el público? ¿Y también tanto para responsables como encargados del tratamiento?
6.– Is privacy by design only for big organizations that process big amounts of personal data?	6.– ¿Es la privacidad por diseño sólo para grandes organizaciones que tratan grandes cantidades de datos personales?
7.– Is privacy by design a competitive advantage for organizations? In particular, how can it help data processors improve their business?	7.– ¿Es la privacidad por diseño una ventaja competitiva para las organizaciones? En particular, ¿cómo puede ayudar a los encargados del tratamiento a impulsar su negocio?
8.– Is privacy a factor to improve innovation or an obstacle? And what is the role of privacy by design for new business models and IT products or services?	8.– ¿Es la privacidad un factor para impulsar la innovación o un obstáculo? ¿Y cuál es el rol de la privacidad por diseño para los nuevos modelos de servicios y productos o servicios basados en la Tecnologías de la Información (TI)?
9.– Do you think data processors are getting a leading role in the development of IT and processing of personal data when providing services that should be taken into closer consideration by competent authorities?	9.– ¿Considera que los encargados del tratamiento están adquiriendo un rol de liderazgo en el desarrollo de TI y el tratamiento de datos personales cuando proporcionan servicios que deberían ser tomados en mayor consideración por las autoridades competentes?
10.– Within an organization, who should be involved when considering and also implementing privacy by design?	10.– Dentro de una organización, ¿quién debería estar involucrado al momento de considerar y también implementar la privacidad por diseño?
11.– How can privacy by design help organizations comply with the law and	11.– ¿Cómo puede ayudar la privacidad por diseño a las organizaciones a cumplir con la

INTERVIEW WITH DR. (PH.D.) ANN CAVOUKIAN, ONTARIO INFORMATION AND PRIVACY COMMISSIONER, ON THE CONCEPT OF PRIVACY BY DESIGN	ENTREVISTA CON LA DRA. ANN CAVOUKIAN, COMISIONADA DE INFORMACIÓN Y PRIVACIDAD DE ONTARIO (CANADÁ), SOBRE LA PRIVACIDAD DESDE EL DISEÑO
regulations on privacy and data protection? And how is privacy by design related to accountability?	normatividad sobre privacidad y protección de datos? ¿Y cómo está relacionada la privacidad por diseño con la rendición de cuentas o responsabilidad ("accountability")?
12.– Two concepts related, how can privacy by design help privacy by default and vice versa?	12.– Dos conceptos relacionados, ¿cómo puede ayudar la privacidad por diseño a la privacidad por defecto y viceversa?
13.– Which have been the big milestones for privacy by design in recent years?	13.– ¿Cuáles han sido los grandes hitos para la privacidad por diseño en los últimos años?
14.– Who are nowadays privacy by design (PbD) ambassadors in Mexico and how can someone become a PbD ambassador?	14.– ¿Quién o quiénes son actualmente los embajadores de la privacidad por diseño en México y cómo se puede ser un embajador de privacidad por diseño?
15.– How do you see the future for privacy by design around the world (Americas –or North America and Latin America-, Europe and APEC)?	15.– ¿Cómo ve el futuro de la privacidad por diseño alrededor del mundo (las Américas –o Norteamérica y Latinoamérica-, Europa y Asia-Pacífico?

5.4 Validación de la Pauta de Entrevista

De acuerdo con los términos de referencia, el 26 de mayo de 2014 se solicitó a la Dirección de Economía Digital de la Secretaría de Economía su opinión sobre el cuestionario en mención, a través del escrito siguiente:

México, D.F., a 26 de mayo de 2014

ASUNTO: Consulta relacionada con el Proyecto: Privacy by design para Fomentar la Figura del Encargado (Procesos 2013)

Lic. OSCAR ISSACHAR BALDERAS ARELLANO
Director Nacional de Fondos y Financiamiento de la CANIETI
Calle Culiacán número 71,
Colonia Hipódromo Condesa, Delegación Cuauhtémoc,
Ciudad de México, Distrito Federal.

LIC. BEATRIZ VELAZQUEZ SOTO
Directora de Economía Digital.
Secretaría de Economía
Av. Insurgentes Sur 194, Cuarto Piso, Colonia Florida,
Ciudad de México, Distrito Federal.

De conformidad con lo establecido con la Fase 2 de la Metodología de los Términos de Referencia (TORs) relacionados con el proyecto "**PRIVACY BY DESIGN PARA FOMENTAR LA FIGURA DEL ENCARGADO (PROCESOS 2013)",** y con el fin de dar cabal cumplimiento a los mismos al momento de reportar a ustedes la **2ª entrega: Segundo Avance**, adjunto al presente nos permitimos poner a su consideración nuestra propuesta de las preguntas (en los idiomas inglés y español) para la entrevista a la **Dra. Ann Cavoukian**, las cuales toman conceptos relacionados con el análisis de los principios del PbD; beneficios de la implementación en las empresas; papel o rol de las Tecnologías de Información; facilidad de implementación en las empresas; casos de éxito desarrollados; retos de la implementación del modelo.

El eje central del cuestionario es tener elementos emanados de la propia autora del concepto de PbD que sirvan como referentes a las MIPYMES del sector de las Tecnologías de la Información (TI) de México para que lo puedan aprovechar o replicar su caso y se fomente el cumplimiento de la normatividad sobre protección de datos personales en el ámbito de las sobre la base.

Debido a que los TORs exigen que para desarrollar la entrevista se requiere el previo acuerdo del Beneficiario y la Secretaría de Economía, les consultamos nuestra propuesta en el sentido de que este cuestionario –una vez validado por Ustedes- le será enviado a la Dra. Cavoukian por correo electrónico, a fin de hacer ágil este proceso; para lo cual requeriremos un mensaje institucional que nos permita establecer el contacto.

Debido a que la 2ª entrega: Segundo Avance **debemos realizarla el 8 de julio**, apreciaríamos su oportuna respuesta.

Sin otro particular, les reiteramos nuestra consideración más distinguida.

Atentamente,

Ing. Belén Leyva Bello
Socia y Representante Legal

CANIETI
CÁMARA NACIONAL DE LA INDUSTRIA ELECTRÓNICA DE TELECOMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN
10 JUN. 2014
RECIBIDO

Paseos de los fresnos 107 interior 601, Colonia Paseos Taxqueña
Delegación Coyoacán, Código Postal 04250, México D.F.
www.gevasesores.com.mx gevasesores@yahoo.com.mx

La validación de este cuestionario por parte de la Secretaría de Economía fue recibida por el Consultor en fecha a 11 de junio a través del siguiente e-mail:

From: blanca.padilla@economia.gob.mx
To: mairalilia@hotmail.com; leyvab@gmail.com
CC: beatriz.velazquez@economia.gob.mx; laura.jimenez@economia.gob.mx
Subject: RE: Cuestionario para Privacy
Date: Wed, 11 Jun 2014 22:00:27 +0000

Hola Maira,
Muchas gracias!! Te comento que ya tuve la oportunidad de revisar el cuestionario con la Lic. Beatriz Velazquez, considerándolo adecuado, únicamente les hacemos los siguientes comentarios:

1- En la pregunta 15, aparentemente habría que replantear la traducción, ya que deberá de referir:
- América
- Norteamérica
- Latinoamérica
- Foro de Cooperación Asía-Pacífico, es decir, las economías miembro de APEC.

Siendo importante también considerar a la:
- Organización para la Cooperación y Desarrollo Económico, es decir, los países miembro de OCDE, en la parte de Europa .

2- Resultando relevante completar otra interrogante enfocada a que detalle las principales consideraciones, recomendaciones, y/o conclusiones respecto al tema.
Por lo que les pedimos toman en cuenta los puntos antes referidos, y dar continuidad a las actividades procedentes.
Cualquier duda o comentario, con mucho gusto la tratamos.

Saludos

Blanca Erika Padilla López
Secretaría de Economía

Dirección General de Innovación, Servicios y Comercio Interior
Dirección de Economía Digital

blanca.padilla@economia.gob.mx
Av. Insurgentes Sur No. 1940, 4° Piso,
Col. Florida, Deleg. Álvaro Obregón,
C.P. 01030 52-29-61-00 Ext. 38105 y 34116

Como consecuencia de las anteriores recomendaciones de la Secretaría de Economía, se modificó la pregunta 15 y se agregó una decimosexta, quedando como sigue:

INTERVIEW WITH DR. (PH.D.) ANN CAVOUKIAN, ONTARIO INFORMATION AND PRIVACY COMMISSIONER, ON THE CONCEPT OF PRIVACY BY DESIGN	**ENTREVISTA CON LA DRA. ANN CAVOUKIAN, COMISIONADA DE INFORMACIÓN Y PRIVACIDAD DE ONTARIO (CANADÁ), SOBRE LA PRIVACIDAD DESDE EL DISEÑO**
15.– How do you see the future for privacy by design around the world, particularly in North and Latin America, and OECD and APEC member countries?	15.– ¿Cómo ve el futuro de la privacidad por diseño alrededor del mundo particularmanente en Norteamérica y Latinoamérica, así como en las Economías de la OCDE y de APEC?
16.- What do you consider are the main challenges Mexico will face on implementing the PbD model? What would be your recommendations for Mexico in order to boost the use of this model?	16.- ¿Cuáles considera son los principales retos que enfrentará México en la implementación del modelo de PbD? ¿Cuáles serían sus recomendaciones para México para poder impulsar este modelo?

5.5 Gestión de la Entrevista con la Dra. Ann Cavoukian

Una vez recibida las anuencias previstas en los Términos de Referencia de este proyecto de parte del Beneficiario (CANIETI) y de la Secretaría de Economía, se procedió a iniciar las pláticas institucionales para identificar el medio para solicitar la entrevista a la Dra. Ann Cavoukian.

Con base en las recomendaciones de la Secretaría de Economía se convino en la elaboración de una carta u oficio (en los idiomas inglés y español) para solicitar formalmente la disposición de la Dra. Cavoukian. Sin embargo, el periodo de consultas internas difirió la gestión, amén de que ella ha cambiado sus datos de contacto con motivo de que su periodo como Comisionada ha finalizado.

El oficio a enviar a través de la Secretaría de Economía, se convino en los siguientes términos:

Como se expuso al elaborar el reporte de la fase 2 del proyecto, las respuestas de la Dra. Cavoukian no se obtuvieron dentro del cronograma previsto en los Términos de Referencia, debido a dos razones:

a) Se requirió un mayor tiempo para que la CANIETI y la Secretaría de Economía pudiesen estar en posibilidades de validar el pliego de preguntas y oficializar la gestión de la entrevista; y

b) Debido a que la Dra. Cavoukian dejó en este mismo año su cargo como Comisionada de la Oficina de privacidad e información de Ontario, Canadá, se requirió de una amplia gestión para localizarla y obtener sus respuestas.

Es de reconocer que cuando fue contactada la Dra. Cavoukian, tanto ella como su equipo de colaboradores mostraron toda la disposición de cooperar en la absolución del cuestionario que elaboró el consultor y le fue enviado de manera oficial por la titular de la Dirección de Economía Digital.

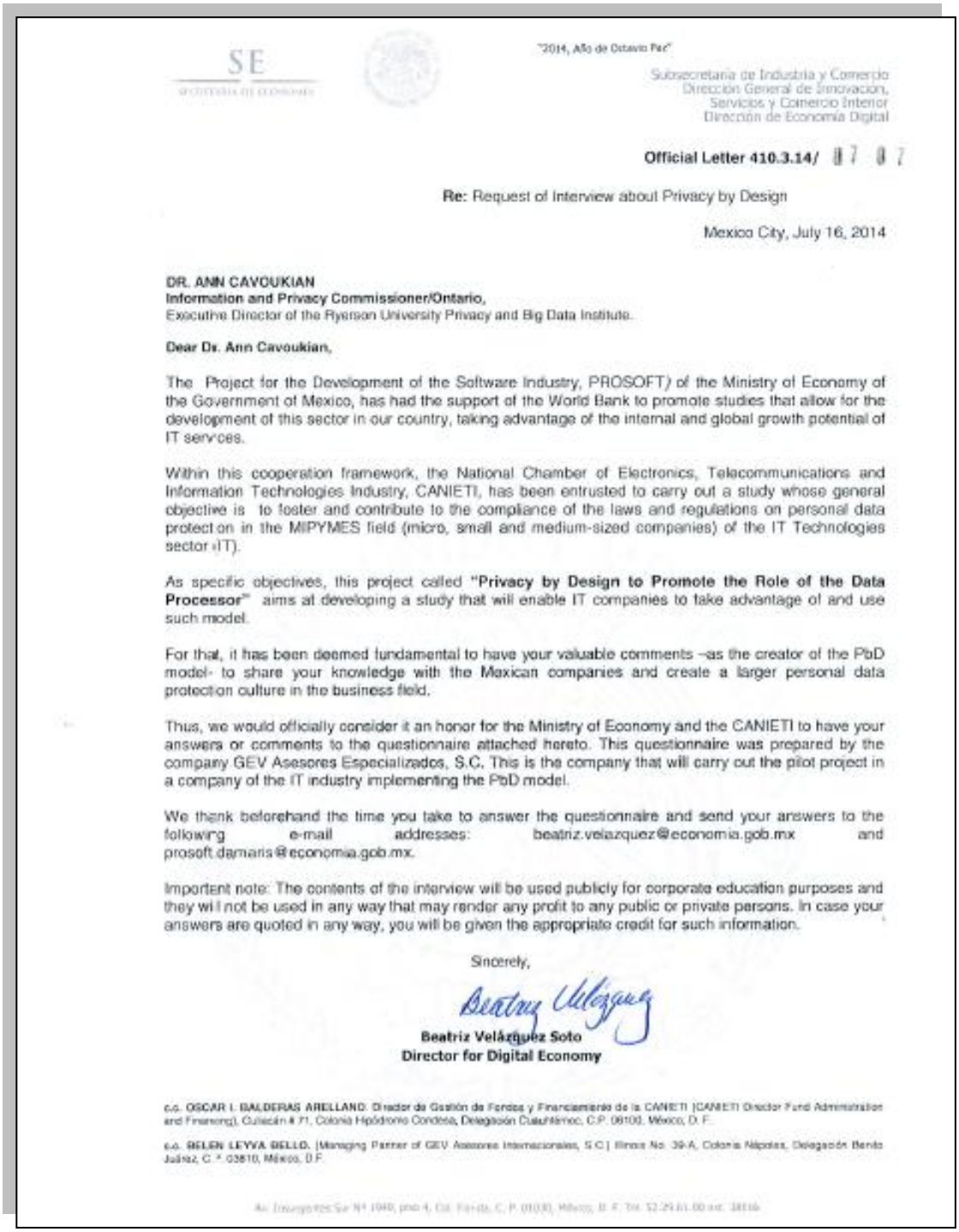
El proceso que se siguió fue el siguiente:

1) **Envío del cuestionario.** Por diversas vías se localizó a la Dra. Cavoukian y finalmente se le envió oficio (oficial letter 410.3.14/0707) y el cuestionario por parte de la Titular de la Dirección de Economía Digital de la Secretaría de Economía el 16 de julio del presente año 2014.

   Actualmente la Dra. Cavoukian es Directora Ejecutiva del Instituto de Privacidad y Big Data (The Privacy and Big Data Institute) en la Universidad de Ryerson[37].

   La carta que se envió formalmente a la Dra. Cavoukian fue la siguiente:

[37] **Ryerson University,** 350 Victoria Street, Toronto, Ontario, M5B 2K3, Main Number: 416.979.5000, www.ryerson.ca



"2014, Año de Octavio Paz"

SE
SECRETARÍA DE ECONOMÍA

Subsecretaría de Industria y Comercio
Dirección General de Innovación, Servicios y Comercio Interior
Dirección de Economía Digital

Official Letter 410.3.14/ 07 07

Re: Request of Interview about Privacy by Design

Mexico City, July 16, 2014

DR. ANN CAVOUKIAN
Information and Privacy Commissioner/Ontario,
Executive Director of the Ryerson University Privacy and Big Data Institute.

Dear Ds. Ann Cavoukian,

The Project for the Development of the Software Industry, PROSOFT) of the Ministry of Economy of the Government of Mexico, has had the support of the World Bank to promote studies that allow for the development of this sector in our country, taking advantage of the internal and global growth potential of IT services.

Within this cooperation framework, the National Chamber of Electronics, Telecommunications and Information Technologies Industry, CANIETI, has been entrusted to carry out a study whose general objective is to foster and contribute to the compliance of the laws and regulations on personal data protection in the MIPYMES field (micro, small and medium-sized companies) of the IT Technologies sector (IT).

As specific objectives, this project called **"Privacy by Design to Promote the Role of the Data Processor"** aims at developing a study that will enable IT companies to take advantage of and use such model.

For that, it has been deemed fundamental to have your valuable comments –as the creator of the PbD model- to share your knowledge with the Mexican companies and create a larger personal data protection culture in the business field.

Thus, we would officially consider it an honor for the Ministry of Economy and the CANIETI to have your answers or comments to the questionnaire attached hereto. This questionnaire was prepared by the company GEV Asesores Especializados, S.C. This is the company that will carry out the pilot project in a company of the IT industry implementing the PbD model.

We thank beforehand the time you take to answer the questionnaire and send your answers to the following e-mail addresses: beatriz.velazquez@economia.gob.mx and prosoft.damaris@economia.gob.mx.

Important note: The contents of the interview will be used publicly for corporate education purposes and they will not be used in any way that may render any profit to any public or private persons. In case your answers are quoted in any way, you will be given the appropriate credit for such information.

Sincerely,

Beatriz Velázquez Soto
Director for Digital Economy

c.c. **OSCAR I. BALDERAS ARELLANO**. Director de Gestión de Fondos y Financiamiento de la CANIETI (CANIETI Director Fund Administration and Financing), Culiacán # 71, Colonia Hipódromo Condesa, Delegación Cuauhtémoc, C.P. 06100, México, D. F.

c.c. **BELEN LEYVA BELLO.** (Managing Partner of GEV Asesores Internacionales, S.C.) Ilinois No. 39-A, Colonia Nápoles, Delegación Benito Juárez, C. P. 03810, México, D.F.

Av. Insurgentes Sur Nº 1940, piso 4, Col. Florida, C. P. 01030, México, D. F. Tel. 52-29-61-00 ext. 38016

2) **Aceptación de la entrevista.** El 18 de julio el Consultor hizo contacto con la Dra. Ann Cavoukian y su asistente (Michael) nos comentó que el día 29 de julio haría llegar las respuestas al cuestionario.
3) **Recepción de respuestas.** El 23 de julio –antes de la fecha ofrecida- se recibió la atenta respuesta vía correo electrónico en la Dirección de Economía

Digital de parte de Renne Barrete, quien es "Assistant Commissioner at the office of the Information and Privacy Commissioner of Ontario"[38], quien tuvo a bien ser conducto para enviar de regreso a México el cuestionario con las respuestas de la Dra. Cavoukian.

5.6 Entrevista a la Dra. Ann Cavoukian

Las respuestas que nos obsequió en el idioma inglés la Dra. Cavoukian se transcriben a continuación y seguidamente la traducción que el consultor realizó al español.

5.6.1. Versión en Inglés (original)

Interview with Ann Cavoukian on the Concept of *Privacy by Design*

1.– What is the meaning of privacy and why it matters? What is your opinion about current issues around the world where privacy is involved? Do you think that privacy is in peril somehow or this is a moment to encourage it?

AC: Privacy is about individual control – maintaining personal control over the collection, use, and disclosure of one's personal data. The right of individuals to assert control over their personal data supports fundamental freedoms and protects against tyranny.

In the information age, privacy has become more essential than ever to protect and promote. For example, big data controlled by government and the private sector can cause many kinds of harms. These harms range from tangible and material harms, such as financial loss, to less tangible harms, such as intrusion into private life and reputational damage.

Privacy is under threat from those who wish to diminish the ability of individuals to participate in the lifecycle of their personal data, and from data controllers and processors who are not fully accountable for their collection, uses and disclosures of personal data.

38 Renee Barrette, Assistant Commissioner (Acting), Tribunal Services Department, Information and Privacy Commissioner/Ontario, 2 Bloor Street East, Suite 1400, Toronto, Ontario M4W 1A8. Email: renee.barrette@ipc.on.ca. Phone: 416-326-3461, Toll Free Phone: 1-800-387-0073, Fax: 416-325-9188, TTY: 416-325-7539

2.– When and why did the IPC create privacy by design? What is the meaning and scope of privacy by design?

AC: Former Commissioner Ann Cavoukian developed *Privacy by Design* in the mid '90s to proactively protect privacy interests by preventing the privacy harm from arising. Not only were fair information practice principles (FIPPs) embedded directly into the design of information technologies and operational processes, they were exceeded through principles such as positive-sum, not zero-sum and privacy as the default setting. Since then, Privacy by Design principles have become universal in scope, and may be applied not only to information technologies, but also to business practices, physical designs, and networked ecosystems. The 7 Foundational Principles of PbD aspire to achieving the highest possible standard of privacy protection. The *Privacy by Design (PbD)* framework advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

3.– Privacy by design as a privacy and data protection principle, how could you explain it for engineers and lawyers at the same time? "Privacy into the code" should be a meeting point for them?

AC: PbD principles build upon, and extend, the traditional FIPPs that currently serve as the basis for privacy laws, policies and practices. One way for engineers and lawyers to conceive of PbD is to think of them as traditional FIPPs that are robustly applied, with added emphasis on being proactive, systematic, and results-oriented.

4.– Do you think that "privacy into the code" could be a starting point also for regulators and legislators?

AC: Efforts to "build privacy into the code" provide credible assurances of an entity's commitment to privacy promises, stronger evidence of regulatory compliance, and best practices for others to emulate.

The OASIS Privacy by Design for Software Engineers (PbD-SE) Technical Committee has developed a draft specification to help document software engineering privacy decisions that are consistent with PbD and the FIPPs.

5.– Is privacy by design both for the private and public sectors? And is it also both for data controllers and data processors?

AC: PbD principles are universal in nature and may be applied by organizations of any size, anywhere, anytime.

6.– Is privacy by design only for big organizations that process big amounts of personal data?

AC: PbD principles have universal application and may be applied equally by app developers and the largest multinational corporations or government entities.

7.– Is privacy by design a competitive advantage for organizations? In particular, how can it help data processors improve their business?

AC: Systematically applying PbD principles in a proactive and creative way typically leads to more efficient and better data management practices. Fewer data breaches, improved customer confidence, trust and lower turn-over, and market recognition of privacy leadership are typical benefits reported by PbD adopters.

8.– Is privacy a factor to improve innovation or an obstacle? And what is the role of privacy by design for new business models and IT products or services?

AC: We have seen no evidence to date that adopting strong privacy practices impedes innovation or limits the success of most business models. Indeed, the evidence to date is that the real obstacle is the failure to appreciate privacy's potential and to apply privacy protections in creative and positive-sum ways.

9.– Do you think data processors are getting a leading role in the development of IT and processing of personal data when providing services that should be taken into closer consideration by competent authorities?

AC: Social, mobile and cloud service providers design and operate platforms of growing ubiquity, complexity, and volumes of personal data. Their activities should be more understandable and accountable to competent authorities.

10.– Within an organization, who should be involved when considering and also implementing privacy by design?

AC: Everyone is responsible for privacy in an organization, but special duties fall to the Chief Privacy Officer, the Board of Directors, and the Executive Suite in general. All organizations should appoint a contact person for privacy.

11. – How can privacy by design help organizations comply with the law and regulations on privacy and data protection? And how is privacy by design related to accountability?

AC:

- PbD reduces chances of human error.
- PbD provides evidence of privacy due diligence (complaint or breach).

Four of the PbD principles promote accountability (to consumers, to regulators, to business partners and shareholders, to team members, and to the public at large).

12.– Two concepts related, how can privacy by design help privacy by default and vice versa?

AC: PbD includes “privacy by default.” Privacy as the Default (Setting) is principle #2, which emphasizes data minimization and other limits on the collection, use, retention and disclosure of personal data, including strong default privacy settings.

13.– Which have been the big milestones for privacy by design in recent years?

AC: In October 2010, PbD was recognized as the global privacy standard in a landmark resolution by the International Conference of Data Protection and Privacy Commissioners in Jerusalem. Since then, the 7 Foundational Principles of PbD have been translated into over 37 official languages.

- Privacy by Design principles have been referenced in U.S. and E.U. regulatory reform proposals.
- Privacy by Design engineering courses are offered at major universities in U.S and E.U.
- International standards Technical Committee (OASIS PbD-SE) approved a draft specification to document PbD in software engineering.
- More than 300 individual and organizational PbD Ambassadors have been appointed.

14.– Who are nowadays privacy by design (PbD) ambassadors in Mexico and how can someone become a PbD ambassador?

AC: We have PbD Ambassadors with connections to Mexico; one in particular is: Cristos Velasco San Martin, Ph.D.

Privacy by Design Ambassadors are an exclusive, but growing, group of privacy thought-leaders committed to ensuring the ongoing protection of personal information by following the Principles of *PbD*. Ambassadors advance the case for embedding privacy protective measures in technology, processes and physical design.

Our practice is to post the names and images of Ambassadors on our *PbD* website, so if the designated ambassador would like to participate in this same recognition, we ask for the following items:

Individual Ambassador

1) High Resolution Headshot Photo
2) Short Bio (200-350 words), highlighting work in privacy and PbD
3) Preferred Mailing Address – We mail a PbD Ambassador Certificate

Organizational Ambassador

1) High Resolution Logo
2) Short Company Description, highlighting work in privacy and PbD
3) Document that outlines how your organization embodies the 7 Foundational Principles

It is important to note that the Information and Privacy Commissioner of Ontario (IPC) is an independent officer of the Legislature whose mandate is to oversee compliance with public sector access and privacy legislation and health sector

privacy legislation in the province of Ontario. The IPC recognizes ambassadors based on their attestations that they apply the principles of Privacy by Design. The IPC does not endorse any company or product of any recognized ambassador.

15.– How do you see the future of privacy by design around the world, particularly in North and Latin America, and OECD and APEC member countries?

AC: Work will continue globally to operationalize the PbD Principles and to establish standards for assessing conformity to those principles in various domains.

16.– What do you consider are the main challenges Mexico will face on implementing the PbD model? What would be your recommendations for Mexico in order to boost the use of this model?

AC: We must never lose sight of the fact that modern privacy is a human right by treating it as an obstacle or inconvenience or equating it to a simple "harm" to be mitigated. Implementing the PbD Model should emphasize individual control and organizational accountability in harmonious balance.

5.6.2 Versión en Español (traducción)

Entrevista con Ann Cavoukian sobre el Concepto de *Privacidad por Diseño*

1.– ¿Cuál es el significado de privacidad y por qué es relevante? ¿Cuál es su opinión sobre los asuntos actuales alrededor del mundo en los que la privacidad está involucrada? ¿Considera que la privacidad está en peligro de alguna manera o que éste es un momento para impulsarla?

AC: La privacidad es acerca del control individual – mantener control personal sobre la recolección, uso y divulgación de nuestros datos personales. El derecho de los individuos a ejercer control sobre sus datos personales apoya libertades fundamentales y los protege de la tiranía.

En la era de la información, proteger y promover la privacidad se ha convertido en un aspecto muy importante. Por ejemplo, las grandes bases de datos controladas por el gobierno y el sector privado pueden causar daño de muchas formas. Estos daños van desde aquellos tangibles y materiales, tales como pérdidas financieras,

hasta daños menos tangibles como intromisión en la vida privada y perjuicio a la reputación.

La privacidad está en peligro por parte de aquellos que desean disminuir la capacidad de los individuos de participar en el ciclo de vida de sus datos personales, y de responsables y encargados de los datos personales quienes no son completamente responsables de su obtención, uso y divulgación de dichos datos personales.

2.– ¿Cuándo y por qué creó usted la privacidad por diseño? ¿Cuál es el significado y alcance de la privacidad por diseño?

AC: La ex comisionada Ann Cavoukian desarrolló *Privacidad por Diseño* a mediados de los 90's para proactivamente proteger los intereses de la privacidad previniendo que el daño a la privacidad aumente. Los principios de prácticas legítimas de la información (FIPPs por sus siglas en inglés) no solamente fueron directamente incluidos en el diseño de tecnologías de la información y de los procesos operacionales, también fueron superados a través de principios tales como de suma-positiva, no de suma-cero y privacidad como configuración por defecto. Desde entonces, los Principios de Privacidad por Diseño se han convertido en principios de alcance universal, y pueden aplicarse no solamente a las tecnologías de información, sino también a prácticas de negocios, diseños físicos y ecosistemas en red. Los 7 Principios Básicos de Privacidad por Diseño (PbD por sus siglas en inglés) aspiran a alcanzar el estándar de protección de privacidad más alto posible. El marco de *Privacidad por Diseño (PbD)* nos da una visión sobre que el futuro de la privacidad no puede asegurarse solamente con el cumplimiento de la legislación y los marcos regulatorios; en su lugar, el aseguramiento de la privacidad debe idealmente convertirse, por defecto, en el módulo de operación de una organización.

3.– Privacidad por diseño como un principio de privacidad y protección de datos, ¿cómo puede explicarlo a ingenieros y abogados al mismo tiempo? ¿Debería ser la "privacidad en el código" un punto de encuentro para ellos?

AC: Los principios de PbD se basaron en y extendieron los FIPPs tradicionales que actualmente sirven como base de las leyes de privacidad, políticas y prácticas. Una manera para los ingenieros y abogados de concebir la PbD es pensar en ellos

como FIPPs aplicadas con firmeza, con énfasis adicional en ser proactivo, sistemático y orientado a resultados.

4.– ¿Considera que la "privacidad embebida en el código" podría ser un punto de partida también para autoridades reguladoras y legisladores?

AC: Los esfuerzos para "construir privacidad en el código" provee seguridad creíble en el compromiso de una entidad en cuanto a las promesas de privacidad, mayor evidencia de cumplimiento regulatorio y para que otros emulen las mejores prácticas.

El Comité Técnico para Ingenieros de Programación Privacidad por Diseño OASIS (PbD-SE por sus siglas en inglés) OASIS Privacy by Design for Software Engineers (PbD-SE) Technical Committee ha desarrollado un borrador de especificaciones para ayudar a documentar las decisiones de privacidad de ingeniería de programación que sean consistentes con la PbD y los FIPPs.

5.– ¿Es la privacidad por diseño tanto para el sector privado como el público? ¿Y también tanto para responsables como encargados del tratamiento?

AC: Los principios de PbD son universales por naturaleza y pueden ser aplicados por organizaciones de cualquier tamaño, en cualquier lugar y en cualquier momento.

6.– ¿Es la privacidad por diseño sólo para grandes organizaciones que tratan grandes cantidades de datos personales?

AC: Los principios de PbD tienen aplicación universal y pueden aplicarse igualmente por desarrolladores de aplicaciones así como por corporaciones multinacionales más grandes o por entidades gubernamentales.

7.– ¿Es la privacidad por diseño una ventaja competitiva para las organizaciones? En particular, ¿cómo puede ayudar a los encargados del tratamiento a impulsar su negocio?

AC: Aplicar sistemáticamente los principios de manera proactiva y creativa lleva generalmente a prácticas de gestión de datos mejores y más eficientes. Menor filtración de datos, mejora en la seguridad del cliente, confianza y menor rotación así como el reconocimiento del liderazgo de la privacidad son beneficios típicos reportados por aquellos que adoptaron PbD.

8.– ¿Es la privacidad un factor para impulsar la innovación o un obstáculo? ¿Y cuál es el rol de la privacidad por diseño para los nuevos modelos de servicios y productos o servicios basados en la Tecnologías de la Información (TI)?

AC: A la fecha no se tiene evidencia de que, adoptar las prácticas de privacidad con firmeza, impida la innovación o limite el éxito de la mayoría de los modelos de negocios. De hecho, la evidencia a la fecha indica que el verdadero obstáculo es el no apreciar el potencial de la privacidad y no adoptar la protección de privacidad de maneras creativas y de suma-positiva.

9.– ¿Considera que los encargados del tratamiento están adquiriendo un rol de liderazgo en el desarrollo de TI y el tratamiento de datos personales cuando proporcionan servicios que deberían ser tomados en mayor consideración por las autoridades competentes?

AC: Los proveedores de servicios sociales, móviles y en la nube diseñan y operan plataformas de creciente localización, complejidad y volúmenes de datos personales. Sus actividades deben ser más entendibles y deben rendir cuentas a las autoridades correspondientes.

10.– Dentro de una organización, ¿quién debería estar involucrado al momento de considerar y también implementar la privacidad por diseño?

AC: Todos somos responsables de la privacidad en una organización, sin embargo tareas en particular recaen en el Oficial Jefe de Privacidad, el Consejo de Directores y el Equipo Ejecutivo en general. Todas las organizaciones deben nombrar una persona de contacto para privacidad.

11.– ¿Cómo puede ayudar la privacidad por diseño a las organizaciones a cumplir con la normatividad sobre privacidad y protección de datos? ¿Y cómo está relacionada la privacidad por diseño con la rendición de cuentas o responsabilidad ("accountability")?

AC:

- PbD reduce los riesgos de un error humano.
- PbD provee evidencia de cumplimiento de debida diligencia de privacidad (queja o filtración).

Cuatro de los principios de PbD promueven la rendición de cuentas (a los consumidores, reguladores, socios de negocios, accionistas, miembros del equipo y al público en general)

12.– Dos conceptos relacionados, ¿cómo puede ayudar la privacidad por diseño a la privacidad por defecto y viceversa?

AC: PbD incluye "privacidad por defecto." Privacidad (Configuración) por defecto es el principio #2, el cual enfatiza minimizar datos y otros límites en la obtención, uso y divulgación de datos personales, incluyendo configuraciones firmes de privacidad por defecto.

13.– ¿Cuáles han sido los grandes hitos para la privacidad por diseño en los últimos años?

AC: En octubre de 2010, PbD fue reconocida como una norma internacional en una resolución emblemática por la Conferencia Internacional de Protección de Datos y Comisionados de Privacidad en Jerusalén. Desde entonces, los 7 Principios Básicos de PbD han sido traducidos a más de 37 idiomas oficiales.

- Las propuestas de reformas regulatorias en EEUU y UE han hecho referencia a los principios de Privacidad por Diseño.
- Cursos de Ingeniería de Privacidad por Diseño se ofrecen en las principales universidades de EEUU y la UE.

- El Comité Técnico de Normas Internacionales (OASIS PbD-SE por sus siglas en inglés) aprobó un borrador de especificaciones para documentar PbD en software de ingeniería.

Más de 300 personas y organizaciones han sido nombrados como Embajadores de PbD.

14.– ¿Quién o quiénes son actualmente los embajadores de la privacidad por diseño en México y cómo se puede ser un embajador de privacidad por diseño?

AC: Tenemos Embajadores PbD con conexiones en México, uno en particular es: Cristos Velasco San Martin, Ph.D.

Los Embajadores de *Privacidad por Diseño* son un grupo de privacidad, exclusivo pero creciente, de líderes de pensamiento comprometidos en asegurar la protección continua de la información personal siguiendo los Principios de PbD Principles of *PbD*. Los Embajadores buscan incluir medidas de protección a la privacidad en tecnología, procesos y diseño físico.

Nuestra costumbre es subir los nombres y las fotografías de los Embajadores en nuestra Página Web de *PbD* website, por lo que, si el embajador designado desea participar en este reconocimiento, solicitamos lo siguiente:

Embajador Individual
1) Una fotografía de su rostro en alta resolución
2) Una corta biografía (entre 200 y 350 palabras), resaltando su trabajo en privacidad y PbD
3) Dirección de Correo principal – Enviamos por correo un Certificado de Embajador PbD

Embajador Organizacional
1) Un logo en alta resolución
2) Una descripción corta de la Empresa, resaltando el trabajo en privacidad y PbD
3) Un documento que resuma como su organización representa los 7 Principios Básicos 7 Foundational Principles.

Es importante resaltar que el Comisionado de Información y Privacidad de Ontario (IPC por sus siglas en inglés) es un Oficial Independiente de la Legislatura, cuyo mandato es supervisar el cumplimiento con la legislación de privacidad y acceso al sector público y la legislación de privacidad en el sector salud en la provincia de

Ontario. El IPC reconoce a los embajadores basados en sus testimonios de que ellos aplican los principios de Privacidad por Diseño. El IPC no respalda ninguna empresa o producto de un embajador reconocido.

15.– ¿Cómo ve el futuro de la privacidad por diseño alrededor del mundo particularmanente en Norteamérica y Latinoamérica, así como en las Economías de la OCDE de APEC?

AC: El trabajo continuará mundialmente para hacer operativos los Principios PbD y establecer los estándares para evaluar el cumplimiento de esos principios en varios ámbitos.

16.- ¿Cuáles considera son los principales retos que enfrentará México en la implementación del modelo de PbD? ¿Cuáles serían sus recomendaciones para México para poder impulsar este modelo?

AC: Nunca debemos perder de vista el hecho de que la privacidad moderna es un derecho humano, y no debemos considerarla como un obstáculo, inconveniente o compararla como un “daño” simple a ser mitigado. La implementación del Modelo PbD debe enfatizar el control individual y la rendición de cuentas organizacional en un balance armonioso.

SEGUNDA PARTE

Implementación piloto y recomendaciones

1. Introducción

Como se señaló en la presentación de esta Entrega Final, la tercera y última fase del proyecto consiste en la realización de un análisis -desde el punto de vista técnico- sobre los beneficios e impactos de insertar el modelo PbD en el desarrollo e implementación de sistemas de información en las empresas.

Para tal efecto, se llevó a cabo la implementación piloto del modelo de PbD en una empresa del Sector de TI a fin de estar en posibilidades de emitir las recomendaciones que sirvan a responsables y encargados del tratamiento para adoptar buenas prácticas a considerar en el diseño o re-diseño de un sistema de información y garantizar así el cumplimiento normativo en protección de datos personales.

2. Selección de la empresa de TI para la implementación piloto del modelo de PbD

De común acuerdo con el Beneficiario (CANIETI) y la Secretaría de Economía, el Consultor procedió a hacer contacto con la empresa que reunía los requisitos para llevar a cabo la implementación piloto del modelo de PbD.

Se trata de una empresa cuyo objeto social principal es la proveeduría de soluciones informáticas. Esta empresa radicada en la Ciudad de México, D.F., está dedicada a prestar servicios de consultoría, administración de proyectos, BPM, y desarrollo e integración de sistemas de información.

Forma Legal: Sociedad Anónima de Capital Variable

Total de Empleados: 900

Para formalizar la invitación a dicha empresa, se le envió la siguiente carta-oficio:

Acuse

México, D.F., a 15 de agosto de 2014

ASUNTO: Invitación a participar en Implementación Piloto del Proyecto *Privacy by Design* para Fomentar la Figura del Encargado (Procesos 2013)

Delegación Cuauhtémoc
México, D.F., C.P. 06600

Por este medio nos permitimos informar que a esta firma consultora le ha sido encomendada la realización del proyecto "**PRIVACY BY DESIGN PARA FOMENTAR LA FIGURA DEL ENCARGADO (PROCESOS 2013)",** impulsado por la Secretaría de Economía a través del PROSOFT 2.0 y el Banco Mundial.

El objetivo general de este proyecto es fomentar y coadyuvar al cumplimiento de la normatividad sobre protección de datos personales en el ámbito de las MIPYMES del sector de las Tecnologías de la Información (TI); y entre sus principales objetivos particulares se encuentran:

- Desarrollar un estudio sobre "Privacy by Design, PbD" que permita a las empresas, en particular a las MIPYMES del sector de TI, aprovechar y aplicar dicho modelo.
- Concientizar a las empresas, sobre los beneficios de la privacidad por diseño y lo que ello supone para el desarrollo de una cultura de protección de datos personales.
- Analizar casos de éxito de la aplicación del modelo y sus beneficios.
- Realizar un proyecto piloto en una empresa del Sector de TI para la implementación del modelo de PbD.

A propuesta de la CANIETI y con la anuencia de la Dirección de Economía Digital de la Secretaría de Economía queremos proponerles que esa empresa participe en la referida implementación piloto, para lo cual les participamos las que su desarrollo busca conseguir los siguientes objetivos:

1. Ayudar a la organización a comprender el alcance de la privacidad por y desde el diseño, de manera que ello le sirva posteriormente para implementar medidas, técnicas, jurídicas y administrativas, para el cumplimiento de la normatividad sobre protección de datos personales y privacidad. Y ello a través de:

    a. Entrevistas y/o uso de un cuestionario elaborado a tal fin que permita obtener información sobre las medidas adoptadas por la organización en relación con la protección de datos de datos personales y la privacidad;
    b. Análisis de información que sea proporcionada por la organización a tal fin, y
    c. Atender dudas o cuestiones que la organización pudiera tener en relación con el concepto de privacidad por diseño, sin que ello suponga la realización de una consultoría o asesoramiento jurídico en materia de protección de datos personales.

Recibí original
Aline Vázquez Ramírez.
21/08/2014.

Paseos de los fresnos 107 interior 601, Colonia Paseos Taxqueña
Delegación Coyoacán, Código Postal 04250, México D.F.
www.gevasesores.com.mx gevasesores@yahoo.com.mx

Limitar el desarrollo del piloto a un periodo de quince (15) días, de manera que la información necesaria pueda obtenerse en tiempo y forma para poder cumplir así con los plazos previstos para este proyecto con la Secretaría de Economía; y

3. Obtener un insumo que sirva para desarrollar recomendaciones sobre el principio de privacidad por y desde el diseño que puedan servir para otras organizaciones, ya sean éstas responsables o encargados del tratamiento.

Alentando contar con su participación, propicio la ocasión para enviarles un cordial saludo.

Atentamente,

Ing. Belén Leyva Bello
Socia y Representante Legal

C.c.p.:

Lic. OSCAR ISSACHAR BALDERAS ARELLANO
Director Nacional de Fondos y Financiamiento de la CANIETI
Calle Culiacán número 71,
Colonia Hipódromo Condesa, Delegación Cuauhtémoc,
Ciudad de México, Distrito Federal.

LIC. BEATRIZ VELAZQUEZ SOTO
Directora de Economía Digital.
Secretaría de Economía
Av. Insurgentes Sur 194, Cuarto Piso, Colonia Florida,
Ciudad de México, Distrito Federal.

Paseos de los fresnos 107 interior 601, Colonia Paseos Taxqueña
Delegación Coyoacán, Código Postal 04250, México D.F.
www.gevasesores.com.mx gevasesores@yahoo.com.mx

3. Trabajo de implementación piloto del modelo de PbD

La fase de implementación piloto del modelo de Privacy by Design dentro de la empresa se dividió, a su vez, en cuatro etapas: 1) Concertación; 2) Levantamiento de Información; 3) Retroalimentación; y 4) Entrega de recomendaciones, las cuales se explican en los siguientes epígrafes.

3.1 Concertación

A fin de precisar los alcances del proyecto en esa empresa, se llevó a cabo una reunión en la sede de su oficina matriz el día 21 de agosto de 2014, en la que estuvieron presentes las siguientes personas:

Participantes

DEPENDENCIA/EMPRESA	Representante
Dirección de Economía Digital de la Secretaría de Economía	Lic. Dámaris
Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI)	Lic. Gisela Rangel y Lic. Dafne Camacho
Empresa	Área legal, de calidad, de proyectos
GEV Asesores Internacionales, S.C.	Ing. Belén Leyva Ing. Flor Hernández

Los temas centrales que se comentaron en dicha reunión de trabajo fueron los siguientes:

- **Tomar en consideración la privacidad por diseño (´*privacy by design*´) desde el inicio:** De manera que la organización que participe en el piloto, desde el principio, ya sea en la fase de diseño de aplicaciones (´*apps*´), su sistema de información o desarrollo del proyecto que se haya propuesto, tome en consideración la necesidad de cumplir con la normatividad sobre protección de datos personales y privacidad.

- **Involucrar a todos los actores relevantes de la organización:** Desde la dirección, que tiene que estar comprometida y facilitar los recursos necesarios, hasta quienes acceden a los datos personales para el desarrollo de sus

funciones, de manera que la protección de datos personales y la privacidad sean un objetivo prioritario.

- **Asegurar el establecimiento de controles y la atención al ejercicio de derechos ARCO:** Al considerar la protección de datos personales y la privacidad desde el inicio, ello permitirá establecer controles para el cumplimiento de la normatividad y el desarrollo de buenas prácticas, así como la atención al ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO), además de la revocación del consentimiento en su caso.

- **Facilitar el cumplimiento de la normatividad sobre protección de datos personales:** La privacidad por y desde el diseño permitirá también facilitar la adopción de medidas para cumplir con el principio de responsabilidad y poder gestionar mejor así el riesgo que implica todo tratamiento de datos personales.

- **Generar confianza de los usuarios a través del cumplimiento y de buenas prácticas en materia de protección de datos personales:** Ya que aplicar los principios de la privacidad desde el diseño ayudará, por una parte, a cumplir con la normatividad sobre protección de datos personales y, por otra parte, a generar confianza por los usuarios, de cualquier lugar del mundo, en productos o servicios que cumplen con altos estándares en materia de protección de datos personales y privacidad.

Acerca del desarrollo del piloto con la empresa, se explicó que se busca conseguir los siguientes objetivos:

a) Ayudar a la organización que participe en el piloto a comprender el alcance de la privacidad por y desde el diseño, de manera que ello le sirva posteriormente para implementar medidas, técnicas, jurídicas y administrativas, para el cumplimiento de la normatividad sobre protección de datos personales y privacidad. Y ello a través de:

  - Entrevistas y/o uso de un cuestionario elaborado a tal fin que permita obtener información sobre las medidas adoptadas por la organización en relación con la protección de datos de datos personales y la privacidad;
  - Análisis de información que sea proporcionada por la organización a tal fin, y

- Atender dudas o cuestiones que la organización pudiera tener en relación con el concepto de privacidad por diseño, sin que ello suponga la realización de una consultoría o asesoramiento jurídico en materia de protección de datos personales.

b) Limitar el desarrollo del piloto a un periodo de quince (15) días naturales, de manera que la información necesaria pueda obtenerse en tiempo y forma para poder cumplir así con los plazos previstos para este proyecto con la Secretaría de Economía;

c) Obtener un insumo que sirva para desarrollar recomendaciones sobre el modelo de privacidad por y desde el diseño que puedan servir para otras organizaciones, ya sean éstas responsables o encargados del tratamiento.

3.2 Levantamiento de información (*Checklists* o cuestionarios sobre *Privacy by Design*)

Una vez explicados los alcances del proyecto a la empresa seleccionada para la implementación piloto, le fue entregado un cuestionario o *checklist* a fin de determinar el grado de cumplimiento de diversos aspectos relacionados con la protección de datos personales.

Dicho pliego de preguntas, fue el siguiente:

Introducción

A través de los presentes *checklists* o cuestionarios sobre la adopción del modelo de privacidad por y desde el diseño (en inglés, *Privacy by Design*, PbD) se quiere conocer cómo la organización ha implementado, en su caso, dicho modelo y algunos aspectos generales en relación con la aproximación que sigue en materia de protección de datos personales y privacidad.

En concreto, lo que se busca es poder obtener una imagen de la situación actual, siendo éste el inicio del piloto en el que [la empresa] está participando de manera que, al finalizar el mismo, ello permita identificar beneficios para la organización en cuanto a considerar el modelo de privacidad por y desde el diseño en los diferentes ámbitos en los que sea aplicable, así como otros aspectos a tomar en consideración para la elaboración de recomendaciones finales que puedan servir

de guía a otras organizaciones que también tratan datos personales, especialmente en el caso de encargados del tratamiento.

En este sentido, la experiencia de [la empresa] será determinante así como, en su caso, las conclusiones que puedan alcanzarse como consecuencia del desarrollo del piloto.

Es así que a continuación se incluyen varios *checklists* o cuestionarios.

1. ***Checklist* o cuestionario para la Junta Directiva, gerente o responsables de departamentos (Jurídico o Legal, Marketing, Tecnologías de la Información, etc.):** Se trata de preguntas que tienen por objeto conocer y determinar el grado de implicación de la organización en cuanto al modelo de privacidad por diseño. Servirán para recabar información que permita indicar en qué estado se encuentra la organización al inicio del piloto así como elaborar posteriormente las recomendaciones del proyecto ante la Secretaría de Economía;

2. ***Checklist* o cuestionario *sobre medidas adoptadas por la organización en materia de privacidad por diseño*:** Son preguntas que están dirigidas a conocer cómo se aplica el modelo de privacidad por diseño en la organización en algún proyecto; quién tiene que implementarlas dentro de la organización, ya sea por parte de ingenieros, asesores legales u otras personas o departamentos que están involucrados en el desarrollo de los proyectos, y

3. **Preguntas finales:** Con las cuales se pueda determinar qué prácticas ha adoptado o piensa adoptar la organización en virtud del piloto e, igualmente, que sirvan para elaborar recomendaciones que puedan ser presentadas a la Secretaría de Economía y, en su caso, sirvan de guía o referente para otras organizaciones.

1.1. Checklist o cuestionario para la Junta Directiva o máximos representantes de la organización

Proyecto: Piloto del proyecto *Privacy by Design* para Fomentar la Figura del Encargado
Nombre de la organización: _____.

Nombre y cargo o puesto de quien responde al cuestionario: _____
Fecha: __ de _____ de 2014

Pregunta 1
Desde la Junta Directiva o al nivel gerencial correspondiente de la organización, ¿se han adoptado medidas para implementar el modelo de privacidad por y desde el diseño de manera que forme parte de las directrices de la organización?
□ Sí; □ No; □ No todavía, pero se está trabajando en ello como uno de los objetivos para este año; □ La protección de datos personales y la privacidad no tienen nada que ver con las actividades que desarrolla la organización y por lo tanto no se han adoptado ni se adoptará medidas al respecto.
Pregunta 2
En caso de respuesta afirmativa a la pregunta anterior, ¿se ha nombrado a una persona o departamento que se encargue de supervisar y reportar a la Junta Directiva los avances sobre el cumplimiento y las correspondientes medidas adoptadas?
□ Sí; □ No; □ No todavía, pero se está en proceso de designar a una persona o departamento.
Pregunta 3
En relación con la pregunta anterior, si se ha designado o se va a designar a una persona o departamento responsable de supervisar la adopción y cumplimiento de medidas en materia de protección de datos y privacidad, ¿se trata de?
□ Una persona física con amplios conocimientos y experiencia en materia de protección de datos personales y privacidad que se dedica únicamente a

esta actividad;

□ El gerente de la empresa. Y de ser así:

○ Tiene conocimientos y experiencia en materia de protección de datos personales;

○ No tiene dichos conocimientos.

□ Un departamento o equipo multidisciplinar (describir en su caso);

□ Es el profesional de gestión de proyectos (*Project Management Professional*, PMP) y/pero:

○ Tiene conocimientos y experiencia en materia de protección de datos personales y privacidad;

○ No tiene dichos conocimientos.

Pregunta 4

¿A quién reporta o reportará, en su caso, la persona o departamento designado conforme a la pregunta anterior?

□ A nadie:

○ Porque se trata del máximo responsable en la materia y únicamente reportará a la Dirección General;

○ No se ha previsto que tenga que reportar a nadie;

○ No se considera necesario que reporte a nadie por no ser una cuestión importante.

□ A la persona o departamento de datos personales;

□ Al gerente;

□ A la Junta Directiva;

□ A la Dirección General.

□ **Importante:** Marque esta casilla si todavía no reporta nadie, pero lo hará en el futuro.

Pregunta 5 *En caso de que sea una persona específica quien vela por las cuestiones relativas a protección de datos y privacidad, ¿con quién colabora?*
□ Con nadie ya que se trata de su responsabilidad gestionar esta cuestión; □ Con un equipo multidisciplinar para tratar cuestiones derivadas de la necesidad de velar por la normativa sobre protección de datos personales y privacidad así como de aspectos derivados de dicho cumplimiento; □ Con el gerente, la Junta Directiva o la Dirección General (especificar quién su caso).
Pregunta 6 *El desarrollo de proyectos en los que se presenten aspectos relativos a la protección de datos personales y privacidad, ¿se lleva a cabo conforme a una metodología como, por ejemplo, PRINCE2, PMP, etc., en la que se tengan en consideración también aquellas cuestiones?*
□ Sí, ¿por qué? □ No. ¿por qué?
Pregunta 7 *¿La privacidad por y desde el diseño se toma en consideración en otras metodologías que en su caso se utilicen en la organización así como en políticas de gestión de riesgos (risk management)?*
□ Sí; □ No.
Pregunta 8 *En su caso, ¿se han incluido referencias al modelo de privacidad por y desde el diseño o a la protección de datos personales en las políticas y otras normas internas de la organización?*
□ Sí; □ No;

□ No todavía, pero es uno de los objetivos previstos para este año.

Pregunta 9

¿Considera a la privacidad por y desde el diseño como un instrumento para generar confianza de todas las partes implicadas, incluidos responsables del tratamiento a los que se presten servicios y, en su caso, los titulares de los datos personales?

□ Sí;

□ No.

Pregunta 10

¿Considera la privacidad por y desde el diseño como parte o relacionado con el principio de responsabilidad (accountability)?

□ Sí;

□ No.

Pregunta 11

¿Se han adoptado medidas para concientizar a todas las personas y actores, internos o externos, implicados en el tratamiento de datos personales para la organización sobre la importancia de aplicar este modelo de privacidad por y desde el diseño?

□ Sí (indique cuál o cuáles):

○ Materiales informativos (*brochures* o folletos, vídeos, área o sección en web corporativa, etc.);

○ Cláusulas contractuales o contratos;

○ Políticas aplicables en cada caso;

○ Otras medidas: _____

□ No;

□ No, pero se está trabajando en ello como uno de los objetivos para este año.

Pregunta 12 *¿Se tienen desarrollados procedimientos y documentos (evidencias) que, en todo momento, permitan responder cuestiones o requerimientos por autoridades competentes en la materia?*
□ Sí; □ No.

Además del *checklist* o cuestionario, si [la Empresa] lo considera oportuno, pueden proporcionar también información o ejemplos prácticos de cómo ha implementado o está implementando y que pueda ser compartida de manera que se cite la fuente correspondiente. Esto es aplicable también al resto de *checklists* o cuestionarios así como a lo largo del desarrollo del piloto.

1.2. Checklist o cuestionario sobre medidas adoptadas por la organización en materia de privacidad por diseño

Proyecto: Piloto del proyecto *Privacy by Design* para Fomentar la Figura del Encargado
Nombre de la organización: _____
Nombre y cargo o puesto de quien responde al cuestionario: _____
Nombre del proyecto: _____
Área encargada:_____
Fecha: ___ de _____ de 2014

Pregunta 1

¿En qué fase se encuentra el proyecto?

□ En diseño;

□ En desarrollo;

□ En operación de 1 a 3 años;

□ Más de 3 años en operación

Pregunta 2

¿A quién va dirigido y, en su caso, qué datos personales se tratan y de quién se recaban los mismos o a través de qué procesos o procedimientos se recaban?

Breve descripción del servicio:

Pregunta 3

En el desarrollo del proyecto, el modelo de privacidad por diseño, ¿se aplica desde la fase inicial y a lo largo de todo el ciclo de vida del proyecto?

□ Sí; □ Solamente al comienzo del proyecto, pero no durante el resto del ciclo de vida del proyecto; □ No; □ No al inicio, pero sí a lo largo del proyecto según las necesidades; □ No, pero se está trabando para adoptar medidas al respecto.
Pregunta 4 *Además del modelo de privacidad por diseño y las políticas de protección de datos personales y privacidad, ¿se aplican otros estándares o principios de protección de datos personales nacionales o internacionales?*
□ Sí, ¿cuáles? □ No.
Pregunta 5 *¿Conoce los principios de privacidad por y desde el diseño de manera que se garantice el derecho fundamental a la protección de datos personales y, al mismo tiempo, se cumpla con la normatividad?*
□ Sí; □ No; □ No actualmente, pero se tomará en consideración.
Pregunta 6 *En la fase de diseño, ¿se consideró realizar evaluaciones de impacto de la privacidad (en inglés, Privacy Impact Assessment, PIA) o evaluaciones similares que permitieran conocer las implicaciones en materia de protección de datos personales y privacidad y tomarlas en consideración?*
□ Sí; □ No; □ No actualmente, pero se tomará en consideración.

Pregunta 7*¿Conoce el aviso de privacidad que maneja su cliente con sus clientes finales?*
□ Sí; □ No.
Pregunta 8 *En caso afirmativo, ¿se hace el tratamiento exclusivamente con base en las finalidades mencionadas en dicho aviso de privacidad?*
□ Sí; □ No.
Pregunta 9 *¿Al inicio del proyecto, se ha tomado en consideración el listado de datos personales que se tratarán?*
□ Sí; □ No; □ No, pero se implementará en futuros proyectos.
Pregunta 10 *¿Se han clasificado (sensibles o no sensibles) los datos personales que se tratan con la finalidad de identificar cómo cumplir con los principios y deberes exigibles en el tratamiento?*
□ Sí; □ No; □ No, pero se implementará en futuros proyectos.
Pregunta 11 *¿Se tratan datos personales de menores de edad en el proyecto?*
□ Sí; □ No.
Pregunta 12 *En caso afirmativo, ¿se han adoptado medidas específicas para cumplir con los principios de información y consentimiento necesario en su caso?*

□ Sí; □ No; □ No, pero se implementará en futuros proyectos.
Pregunta 13 *¿Se tratan datos personales sensibles en el proyecto (relativos a salud, creencia religiosa, etc.)*
□ Sí; □ No.
Pregunta 14 *En caso de que se traten datos personales sensibles ¿se ha tomado en consideración la protección de los mismos desde el inicio para cumplir con los principios y deberes específicos aplicables?*
□ Sí; □ No; □ No, pero se implementará en futuros proyectos. □ No se tratan datos personales sensibles.
Pregunta 15 *¿Es el cliente quién determina en todo momento qué datos personales se recaban y con qué finalidad se tratan?*
□ Sí; □ No, ya que en ocasiones el cliente no sabe exactamente qué datos personales se trata.
Pregunta 16 *En este proyecto, ¿se han identificado qué medidas de seguridad es necesario adoptar en cada tratamiento de datos personales?*
□ Sí;

□ No;

□ No actualmente, pero se tomará en consideración.

Pregunta 17

¿Tiene firmado un contrato u otro instrumento jurídico (cláusula contractual, convenio, anexo a un contrato) de prestación de servicios relativo al tratamiento de datos personales con su cliente?

□ Sí;

□ No.

Pregunta 18

En caso afirmativo, favor de marcar los temas que se incluyen dentro de las cláusulas contractuales:

□ Conocimiento y aplicación de políticas de protección de datos personales de acuerdo a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento;

□ Hacer del conocimiento del cliente las subcontrataciones necesarias para llevar a cabo la prestación de los servicios;

□ Limitar la propiedad de la información sobre la que se prestan los servicios;

□ Guardar confidencialidad respecto de los datos personales sobre los que se presta el servicio;

□ Cuenta con herramientas para dar a conocer los cambios en sus políticas de privacidad a su cliente;

□ Medidas de seguridad administrativas para la protección de datos personales;

□ Medidas de seguridad físicas para la protección de datos personales;

□ Medidas de seguridad técnicas para la protección de datos personales;

□ Mecanismos de supresión de los datos personales una vez concluidos los servicios contratados previa recuperación de dichos datos por parte del cliente.

Pregunta 19 *Adicionalmente, en este proyecto, ¿se establecen controles (contratos con terceros, cláusulas con empleados, etc.) que permitan evaluar y garantizar el cumplimiento de los principios de protección de datos y la privacidad?*
□ Sí; □ No; □ No actualmente, pero se tomará en consideración..
Pregunta 20 *En caso de respuesta afirmativa a la pregunta anterior, ¿se mide el grado de cumplimiento conforme a los objetivos establecidos en el plan o documento de diseño del proyecto en materia de protección de datos personales para identificar brechas o faltantes así como objetivos que se cumplen?*
□ Sí; □ No; □ No actualmente, pero se tomará en consideración.
Pregunta 21 *En relación con los avances y cuestiones que se plantean en materia de protección de datos personales y privacidad a lo largo del proyecto, ¿se comunica a los responsables de los departamentos o supervisores del proyecto la existencia de puntos débiles para la adopción de medidas correctivas?*
□ Sí; □ No; □ No actualmente, pero se tomará en consideración.
Pregunta 22 *¿Consideran en el futuro auditar el proyecto para para determinar el grado de cumplimiento en materia de protección de datos personales y privacidad?*
□ Sí, por auditores internos;

□ Sí, por auditores externos; □ No.
Pregunta 23 *El proyecto, por lo que se refiere al tratamiento de datos personales, ¿será objeto de alguna certificación o cumplirá con algún código de conducta, ético o similar?*
□ Sí, se obtendrá una certificación (indicar cuál si ya se conoce); □ Sí, cumple con un código de conducta (indicar cuál); □ No.
Pregunta 24 *Si su cliente le encomienda algún servicio que implique el tratamiento de datos personales o tratamiento que no cumpla con la normatividad aplicable, ¿le avisa sobre dicha circunstancia?*
□ Sí; □ No.

1.3. Preguntas finales

Proyecto: Piloto del proyecto *Privacy by Design* para Fomentar la Figura del Encargado
Nombre de la organización: _____
Nombre y cargo o puesto de quien responde al cuestionario: _____
Fecha: ___ de _____ de 2014

Pregunta 1

En caso de que la privacidad por diseño sea considerada como un aspecto positivo *¿Se ve a la privacidad por diseño como una ventaja competitiva con respecto a otras organizaciones que no la tienen en consideración?*

□ Sí (explique brevemente por qué);

□ No (explique brevemente por qué).

Pregunta 2

El desarrollo de proyectos conforme al modelo de privacidad por diseño, ¿permite obtener información y buenas prácticas que puedan ser utilizadas en futuros proyectos?

□ Sí;

□ No;

□ No se ha tomado en consideración hasta la fecha, pero se hará en el futuro.

Pregunta 3*En su caso, ¿puede decirnos si el piloto le ha aportado información o le ha planteado cuestiones, y en su caso cuáles, que tendrá en consideración para futuros proyectos en cuanto a la implementación del modelo de privacidad por diseño?*

□ Sí, ¿cuáles?

□ No me ha aportado nada.

ADVERTENCIA:

Las respuestas textuales obtenidas por el consultor de parte de la empresa no se plasman en este reporte debido al convenio de confidencialidad y reserva de la información celebrado entre ambos.

3.3 Retroalimentación

Una vez recibidas las respuestas de parte de la empresa participante en la implementación piloto del modelo de PbD, se llevó a cabo una reunión de trabajo el día 2 de septiembre para aclarar diversos aspectos.

De dicha reunión resultaron los siguientes aspectos:

La empresa seleccionada por la CANIETI en conjunto con la Secretaría de Economía para participar en la prueba piloto manifestó ser una empresa que pertenece al sector de TI y uno de los servicios que presta, hasta el momento, lo hace como encargado de tratamiento de datos personales.

La organización en mención no tenía conocimientos sobre el modelo de privacidad por diseño, sin embargo, sí toma como base la normatividad mexicana en materia de privacidad y protección de datos personales al momento de llevar a cabo algún tipo de servicio que involucre este tipo de datos. Asimismo, cuenta con un equipo multidisciplinario formado por cinco personas pertenecientes a las áreas de legal, administración y finanzas, calidad, sistemas y proyectos para supervisar la adopción y cumplimiento de medidas en materia de protección de datos y privacidad y el cual reporta a la Junta Directiva.

El proyecto que se seleccionó para el levantamiento de cuestionarios y *checklists* fue una solución que prestan a empresas que requieren el envío y recepción masivo de información a sus clientes mediante mensajes por diferentes medios electrónicos. Es un servicio que lleva más de tres años operando siendo una solución a través de la cual se lleva a cabo tratamiento de datos personales de los clientes finales, sin embargo, desconoce la forma de obtención de estos datos por parte de su cliente.

El tratamiento de datos personales se lleva a cabo de acuerdo a las finalidades establecidas por el cliente y conforme al aviso de privacidad del mismo, que se encuentra en su página Web, entre otros medios. Este servicio está sujeto a un contrato de prestación de servicios que contempla dentro de sus cláusulas tanto medidas de seguridad como el tema de la confidencialidad. Para poder proveer el servicio a un cliente nuevo se sigue un procedimiento en el área legal y en el área técnica. Adicionalmente se cuenta con una serie de controles que buscan evaluar el grado de cumplimiento de los principios de protección de datos personales y la privacidad mediante auditorías internas, de tal forma que sea posible identificar brechas y posteriormente adoptar medidas correctivas de los puntos débiles identificados.

Respecto a la inducción, formación y capacitación que se contempla dentro del modelo de privacidad por diseño, esta empresa tiene un programa de cursos de inducción para nuevos empleados y de formación y de capacitación para los existentes de tal forma que entre los temas que se cubren se encuentra el relacionado con la protección de datos personales.

Es importante señalar que la empresa cuenta con un código de ética que si bien contempla el tema de la confidencialidad aún carece de algún apartado sobre privacidad y protección de datos personales.

Finalmente, la empresa mencionó que una buena práctica será implementar este modelo en proyectos futuros y en los existentes.

4. Análisis de los beneficios e impactos de la inserción del Modelo de PbD en las empresas de TI

Insertar el modelo de privacidad por o desde el diseño (*privacy by design*, PbD) en el desarrollo e implementación de sistemas de información en organizaciones, modelos o prácticas de negocio y en el diseño físico e infraestructura, tiene importantes beneficios e impactos positivos para aquéllas, bien sean responsables o bien sean encargados del tratamiento, y también para las personas cuyos datos personales son tratados, ya que el modelo de privacidad por diseño puede ser un instrumento a través del que se catalice el cumplimiento, en la medida en que el mismo implica adoptar e implementar medidas para garantizar la protección de datos personales en todo tratamiento personales que lleve a cabo. Al mismo tiempo, dicho principio implica también un importante factor de concientización al interior de la organización.

A continuación, se tratan los puntos relevantes a los que da lugar un análisis en la práctica del modelo de privacidad por diseño, apoyando dicho análisis en los resultados obtenidos del programa piloto que se ha llevado a cabo como parte del presente proyecto.

Se han tomando en consideración también otros aspectos y factores relevantes que permiten concluir que, en relación con dicho principio, es necesario seguir trabajando con una programa específico que abarque todos los ámbitos, desde políticas públicas por las autoridades reguladoras, como la Secretaría de Economía, hasta que las empresas sean conscientes de la necesidad de adoptar e implementar medidas en la práctica, si se quieren obtener los máximos beneficios.

Derivado de dicho análisis, es posible presentar a continuación varios puntos relevantes:

- **El concepto de privacidad por diseño es amplio pero suficientemente preciso:** Es necesario recordar que el concepto sigue vigente dos décadas después de que fuera acuñado a mediados de los años 90 por la Dra. Ann Cavoukian, entonces Comisionada de la Oficina de privacidad e información de Ontario, Canadá, y que el mismo abarca diferentes casos (desarrollo e implementación de sistemas de información en organizaciones, modelos o prácticas de negocio y en el diseño físico e infraestructura), y aplica a

cualquier tipo de organización, con independencia de su tamaño y área de actividad, así como *"en cualquier lugar y en cualquier momento"* tal y como señaló la Dra. Ann Cavoukian. Por lo tanto, es necesario pensar en el principio también como una filosofía, en cuanto a que a través del mismo es posible concientizar a las organizaciones, ya sean responsables o encargados del tratamiento, de la necesidad de adoptar e implementar medidas para cumplir con los principios y deberes previstos en la normatividad sobre protección de datos personales.

- **El modelo de privacidad por diseño ha sido reconocido a nivel internacional tanto por las autoridades de protección de datos personales como por la normativa:** Siendo buena muestra de ello el hecho de que las autoridades de protección de datos personales y privacidad a través de la Resolución sobre Privacidad por Diseño, adoptada durante la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que se celebró en Jerusalén, Israel, durante los días 27 a 29 de Octubre de 2010, a la que ya nos hemos referido. También, varias autoridades de protección de datos personales alrededor del mundo, como por ejemplo, Reino Unido, Alemania y Australia o la Comisión Federal de Comercio (*Federal Trade Commission*, FTC) de los Estados Unidos de América, han adoptado guías en relación con el modelo de privacidad por diseño. Además, el Supervisor Europeo de Protección de Datos (SEPD) ha hecho referencia en varios de sus dictámenes al modelo de privacidad por diseño. Por último, en el caso de la Unión Europea, pueden encontrarse referencias al citado principio a nivel normativo en la Recomendación 2012/148/UE de la Comisión, de 9 de marzo, relativa a los preparativos para el despliegue inteligente de los sistemas de contador inteligente, ya citada; así como que en, el todavía futuro, Reglamento general de protección de datos, al que también nos hemos referido, se incluye un artículo que hace referencia de manera específica al modelo de privacidad por diseño.

- **En México no se encuentran referencias al modelo de privacidad por diseño:** Ni la normatividad sobre protección de datos personales, la LFPDPPP y su Reglamento, ni las autoridades competentes en la materia, principalmente el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y las autoridades reguladoras, se han referido al modelo de privacidad por diseño, siendo este análisis de la Secretaría de Economía el primero que presta atención, tanto de forma teórica como práctica, al

mismo. Lo anterior debe servir para continuar el camino que se inicia con este estudio, en cuanto a profundizar sobre este principio y cómo aplicarlo, en su caso, en el caso de México.

- **No hay métricas sobre el modelo de privacidad por diseño:** Analizar en el impacto en la práctica del modelo de privacidad por diseño resulta complejo, de igual manera que ocurre en el caso del impacto y cumplimiento de la normatividad en materia de protección de datos personales en general y en otras áreas. De las respuestas que amablemente dio la Dra. Ann Cavoukian a la entrevista hecha durante este proyecto, cabe resaltar que en relación con este principio *"[a]plicar sistemáticamente los principios de manera proactiva y creativa lleva generalmente a prácticas de gestión de datos mejores y más eficientes. Menor filtración de datos, mejora en la seguridad del cliente, confianza y menor rotación así como el reconocimiento del liderazgo de la privacidad son beneficios típicos reportados por aquellos que adoptaron PbD."* Esto significa que deban, en su caso, desarrollarse métricas para medir los niveles de cumplimiento y, en su caso, incumplimiento de los principios y, también, de la normatividad aplicable.

- **El modelo de privacidad por diseño todavía está en evolución:** Entre las razones para no encontrar métricas concretas, debe atenderse a que una de las respuestas dadas por la Dra. Ann Cavoukian en la entrevista fue *"El trabajo continuará mundialmente para hacer operativos los Principios PbD y establecer los estándares para evaluar el cumplimiento de esos principios en varios ámbitos."* La respuesta representa una oportunidad para México, que podría adoptar medidas para adoptar los principios de privacidad por diseño o, en su caso, desarrollar métricas específicas conforme a los principios que estime oportunos. Al respecto, sería relevante tomar en consideración que el IFAI realizó en 2012 una Encuesta Nacional de Protección Datos Personales[39], realizando un seguimiento periódico o realizando nuevas encuestas que permitan medir el nivel de conocimiento y cumplimiento de la normatividad sobre protección de datos personales especialmente dirigidas a responsables y encargados del tratamiento.

[39] Los informes y resultados a los que dio lugar la citada encuesta pueden encontrarse en el vínculo electrónico http://inicio.ifai.org.mx/_catalogs/masterpage/Encuesta-Nacional-de-Proteccion-de-Datos-Personales-2012.aspx

- **El modelo de privacidad por diseño es desconocido en México:** El programa piloto llevado a cabo como parte del presente proyecto ha supuesto explicar y concientizar a la empresa que amablemente aceptó participar, siendo relevante el hecho de que la misma tenga un alto nivel de cumplimiento de la normatividad sobre protección de datos personales, si bien el modelo de privacidad por diseño resulta novedoso para la misma siendo una cuestión sobre la que la empresa desea trabajar para aumentar las medidas que ya ha adoptado hasta el presente.

- **Es necesario dar visibilidad a los análisis y materiales de la Secretaría de Economía:** A pesar de que durante los últimos años la Secretaría de Economía viene desempeñando una importante labor, atendiendo específicamente a promover la figura del encargado del tratamiento, los resultados pueden no estar siendo aprovechados por los responsables y encargados del tratamiento, siendo un ejemplo el caso de la empresa que ha participado en el programa piloto objeto de este proyecto, la cual no está familiarizada con las funciones de la Secretaría de Economía y para la que también sería deseable contar con una guía o más información sobre el modelo de privacidad por diseño, siendo ésta una cuestión sobre la que la Secretaría de Economía podría considerar el insumo que representa el análisis hecho para generar dicha guía o adoptar otras medidas que permita explotar al máximo el trabajo que se ha realizado y que sirva en la práctica para que las organizaciones se beneficien del mismo.

- **A la hora de ponerlo en práctica, el modelo de privacidad por diseño debe considerarse a la luz de los principios y deberes de la LFPDPPP y su Reglamento:** Lo que supone que deba atenderse tanto a los principios y deberes, especialmente por lo que se refiere a las medidas a adoptar en virtud del principio de responsabilidad y sobre el resto de principios, como otras obligaciones previstas en la normatividad, tales como la designación de una persona o departamento de datos personales, que puede ser además la figura clave para velar o apoyar que se implemente este modelo de privacidad por diseño, siendo además un aspecto o cuestión sobre la que se requiere el impulso por parte de la Secretaría de Economía, otras autoridades garantes y, en última instancia, el IFAI.

5. Recomendaciones

Las recomendaciones en materia del modelo de privacidad por diseño (*privacy by design*, PbD), se dirigen tanto a la Secretaría de Economía, en su papel de autoridad reguladora, como a los responsables y encargados del tratamiento, quienes están sujetos al cumplimiento de la normatividad sobre protección de datos personales.

El papel que desempeñe la Secretaría de Economía, como autoridad reguladora, con respecto al modelo de privacidad por diseño, es fundamental, ya que de ello puede depender que dicho modelo se materialice en la realidad, al facilitar a responsables y encargados del tratamiento orientación sobre el mismo de manera que puedan aprovecharse las ventajas que ofrece y ser también una metodología que permita distinguir claramente el desarrollo de tecnología y servicios que cumplan con protección de datos personales y privacidad.

Al mismo tiempo, los responsables y encargados del tratamiento pueden encontrar en el modelo de privacidad por diseño un instrumento adecuado tanto para implementar medidas que permitan garantizar el cumplimiento de la normatividad sobre protección de datos personales, como una filosofía que permita implementar buenas prácticas en todas las áreas de la organización, así como divulgar el conocimiento de este derecho fundamental entre todas las personas implicadas en el tratamiento de datos personales en las operaciones diarias.

5.1. Dirigidas a la Secretaría de Economía

La implementación y, en su caso, cumplimiento del modelo de privacidad por o desde el diseño no es sólo una cuestión que incumba a los responsables y encargados del tratamiento, sino que requiere también de la adopción de medidas por las autoridades competentes que, en materia de protección de datos personales en posesión de los particulares, son tanto el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), en su papel de autoridad garante, como la Secretaría de Economía, en el desarrollo de sus funciones como autoridad reguladora.

En concreto, la LFPDPPP, en su artículo 43, encomienda a la Secretaría de Economía, entre otras, las atribuciones relativas a:

- *Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial* (fracción I);

- *Fomentar las buenas prácticas comerciales en materia de protección de datos personales* (fracción II);

- *Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales* (fracción VIII), y

- Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales (fracción X).

Dichas funciones son clave para apoyar en la práctica la adopción e implementación del modelo de privacidad por o desde el diseño en México.

En concreto, a la vista de la evolución del modelo de privacidad por diseño desde que fue acuñado en los años 90 por la Dra. Ann Cavoukian, el reconocimiento de dicho modelo a nivel internacional, sería recomendable que la Secretaría de Economía, como autoridad reguladora y con atribuciones en materia de protección de datos personales en el ámbito comercial, pudiera:

1. Desempeñar una labor de concientización dirigida a los responsables y encargados del tratamiento, así como en su caso a otros sujetos tanto del sector privado como del sector público involucrados en promover el derecho fundamental a la protección de datos personales, con la finalidad de que el modelo de privacidad por o desde el diseño sea adoptado e implementado por los responsables y encargados del tratamiento;

2. Divulgar información sobre el modelo de privacidad por diseño como un instrumento adecuado que permita elaborar un plan de acción tomando en consideración la protección de datos personales y la privacidad desde la fase más temprana de diseño y desarrollo de la arquitectura de los sistemas de tecnologías de la información y prácticas de negocio;

3. Fomentar la adopción e implementación del modelo de privacidad por diseño como una buena práctica en el ámbito comercial, siendo éste en el

que se produce una gran parte de avances tecnológicos[40] que requieren ser desarrollados conforme a dicho modelo para garantizar así la protección de datos personales y la privacidad;

4. Diseñar e instrumentar políticas públicas cuya finalidad sea el conocimiento por los responsables y encargados del tratamiento, en el ámbito comercial, de las obligaciones que tienen a la hora de tratar datos personales, incluyendo la conveniencia de implementar el modelo de privacidad por diseño;

5. Realizar eventos con la participación de todos los actores involucrados en materia de protección de datos personales, con la finalidad de dar a conocer el modelo de privacidad por diseño, sus beneficios e implicaciones para el desarrollo de servicios y tecnologías que cumplan con la protección de datos personales, lo que a su vez puede convertirse en un elemento que sirva para generar confianza de los usuarios;

6. Apoyar la elaboración de estudios y monitoreo de avances que se produzcan a nivel internacional sobre el modelo de privacidad por diseño[41], de manera que México aproveche la experiencia acumulada a nivel internacional y la pueda transformar en buenas prácticas de las que se beneficien los responsables y encargados del tratamiento que tienen que cumplir con la normatividad sobre protección de datos personales;

7. Apoyar, en el ámbito de sus competencias, la adopción de medidas que tengan por objeto la adopción e implementación del modelo de privacidad por diseño a nivel nacional, de manera que pueda plasmarse en políticas públicas, lineamientos u otros instrumentos que sean vinculantes para responsables y encargados del tratamiento;

[40] Como ejemplo, cabe citar que según Gartner, la firma especializada en TI, México se convertirá en el principal país de Latinoamérica que proporcione servicios de centros de datos para 2018, tratándose de un mercado que en 2014 tendrá un valor a nivel global de USD 143,000 millones. La referencia a esta cifra puede verse en http://eleconomista.com.mx/tecnociencia/2014/08/12/ven-menor-dinamismo-industria-ti-2014 [disponible el 5 de septiembre de 2014].

[41] Por ejemplo, en el caso de la Unión Europea, una de las novedades del futuro Reglamento general de protección de datos es la inclusión del principio de privacidad por diseño como una de las obligaciones del responsable del tratamiento, en el artículo 23. La propuesta puede verse en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012PC0011&rid=1 [disponible el 5 de septiembre de 2014].

8. Divulgar, a través de los instrumentos y/o foros o eventos oportunos, la interrelación del modelo de privacidad por diseño con los principios de la protección de datos personales, y en particular, con el principio de responsabilidad o rendición de cuentas, así como el papel que puede desempeñar al respecto la persona o departamento de datos personales[42];

9. Fomentar la inclusión del modelo de privacidad por diseño en esquemas de autorregulación en materia de protección de datos personales, aprovechando a tal fin los Parámetros de Autorregulación en materia de Protección de Datos Personales[43];

10. Educar a responsables y encargados del tratamiento sobre los beneficios que implica el modelo de privacidad por diseño, tanto por lo que se refiere a garantizar el cumplimiento de la normatividad sobre protección de datos personales, lo que permite reducir el riesgo derivado del tratamiento y uso de datos personales, así como que se trata de una buena práctica de negocio, que debe regir todos los tratamientos de datos personales, y

11. Actuar en coadyuvancia con el IFAI buscando áreas de oportunidad en las que sus acciones puedan tener la mayor repercusión e impacto posibles, con la finalidad de que la implementación de modelos como el de privacidad por diseño u otras acciones redunden en beneficio tanto de los responsables y encargados del tratamiento como de las personas cuyos datos personales son tratados, lo que a su vez permitirá a México ser un ejemplo a seguir por sus socios comerciales y otros países.

5.2 Dirigidas a responsables y encargados del tratamiento

En el caso de los responsables y encargados del tratamiento, quienes tienen que adoptar medidas para cumplir con las obligaciones que les son exigibles conforme a la LFPDPPP, su Reglamento y demás normatividad aplicable, es necesario que éstos puedan contar con una regulación clara, que a su vez pueda ser complementada por la autorregulación.

En concreto, el modelo de privacidad por o desde el diseño, permitirá a los responsables y encargados del tratamiento, cumplir desde el inicio con la

[42] Tal y como prevé la LFPDPPP en su artículo 30, ya que entre las funciones de esta persona o departamento de datos personales está la de fomentar *"la protección de datos personales al interior de la organización."*
[43] Publicados en el Diario Oficial de la Federación el 29 de mayo de 2014.

normatividad y requisitos en materia de protección de datos personales, lo que supone minimizar el riesgo de sanción; otros riesgos, como por ejemplo la pérdida de confianza por parte de potenciales clientes, clientes o accionistas, autoridades administrativas y judiciales competentes; así como embeber o incorporar los principios de protección de datos personales y privacidad en todas las áreas y acciones de la organización.

Es por ello que a la hora de implementar o incorporar el modelo de privacidad por diseño, la organización tiene que ser activa, partiendo del hecho de que dicho modelo está estrechamente interrelacionado con el cumplimiento de las obligaciones que tiene la misma en el cumplimiento de la normatividad sobre protección de datos personales ya sea como responsable o encargado del tratamiento[44].

Además de conocer el significado y alcance del modelo de privacidad por diseño, pudiendo desempeñar la persona o departamento de datos personales un papel relevante al respecto, cualquier responsable o encargado del tratamiento que trate datos personales, debe contar con un *roadmap* o plan de acción a través de la que se tome en consideración el modelo de privacidad por diseño a la hora de adoptar medidas para cumplir con la normatividad sobre protección de datos personales.

Una propuesta de *roadmap* o plan de acción al respecto podría ser la siguiente, siendo condición previa necesaria que el responsable o encargado del tratamiento tenga una posición proactiva al cumplimiento, lo que implica aportar recursos necesarios, cualquiera que sea su naturaleza (materiales, humanos, financieros, etc.), considerando el cumplimiento de la protección de datos personales como una ventaja competitiva[45].

Sobre esta cuestión, puede verse la Encuesta Nacional de Protección de Datos Personales 2012, elaborada por el IFAI, y conforme a la cual se puede concluir que la percepción de la mayoría de las empresas que participaron en la misma es que la mayoría (76%) *"considera que la LFPDPPP tiene muchísima o mucha utilidad"*. Ahora bien, es necesario tomar en consideración que la realidad es que

[44] En relación con el cumplimiento de dichas obligaciones, no puede olvidarse que el IFAI ha emitido diversas guías, entre las que destaca aquí la *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, disponible en la dirección de Internet http://inicio.ifai.org.mx/_catalogs/masterpage/ifai.aspx [consultada el 5 de septiembre de 2014].

[45] La citada encuesta está disponible en la dirección de Internet http://inicio.ifai.org.mx/EncuestaNacionaldeProteccciondeDatosPersonales2012/02ReporteEmpresas.pdf [consultada en fecha 5 de septiembre de 2014].

el *"84% de las empresas desconoce las obligaciones derivadas de la entrada en vigor de la LFPDPPP."*

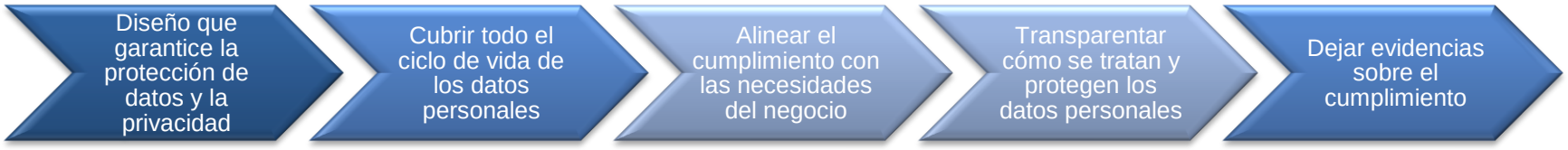
En la práctica, el modelo de privacidad por diseño implica:

Para su aplicación en la práctica, el modelo de privacidad por diseño puede resumirse de la siguiente forma:

Modelo de privacidad por o desde el diseño (privacy by design, PbD)[46]		
Aplica a	Datos personales:	Todos los tipos de datos personales
	Organizaciones:	Cualquier tipo de organización
	Ámbitos:	• Sistemas de tecnologías de la información • Prácticas de negocio responsables *(compliance)* • Diseño físico e infraestructura en red
Atiende a	Sensibilidad de los datos, considerando su naturaleza	
Objetivos	1) Garantizar la privacidad, y 2) Ser una ventaja competitiva sostenible.	
Principios	1) ***Proactivo***, no Reactivo; ***Preventivo*** no Correctivo 2) Privacidad como la ***Configuración Predeterminada*** 3) Privacidad ***Incrustada*** en el Diseño 4) Funcionalidad Total – ***"Todos ganan"***, no "Si alguien gana, otro pierde" 5) Seguridad Extremo-a-Extremo – ***Protección de Ciclo de Vida Completo*** 6) ***Visibilidad*** y ***Transparencia*** – Mantenerlo ***Abierto*** 7) ***Respeto*** por la Privacidad de los Usuarios – Mantener un Enfoque ***Centrado en el Usuario***	

[46] Véase Privacy by Design, Los 7 Principios Fundamentales. Disponible en la dirección de Internet http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf [consultada el 6 de septiembre de 2014].

Con carácter general, las medidas a adoptar y adoptadas en virtud del modelo de privacidad por o desde el diseño, conforme a la responsabilidad de cada área de la organización, deben dar lugar a su vez a conseguir los siguientes objetivos:



En relación con el modelo de privacidad por diseño, por cada una de las áreas de la organización, así como en su caso otras partes interesadas, tales como la autoridad garante y las autoridades reguladoras, es posible presentar la siguiente propuesta de *roadmap* o plan de acción, dirigida a responsables y encargados del tratamiento para que les sirva al momento de adoptar buenas prácticas a considerar en el diseño o re-diseño de un sistema de información y garantizar así el cumplimiento normativo en protección de datos personales, es la que se incluye a continuación:

Roadmap o plan de acción general para la implementación del modelo de privacy by design

1 Dirección de la organización	2 Gerencia	3 Desarrollo (tecnológico o de otra naturaleza, por ejemplo, marketing u operaciones) y cumplimiento (TI & Legal)
• Proporcionar el apoyo y recursos necesarios para que el cumplimiento de la normatividad sobre protección de datos y privacidad sean los ejes rectores de cualquier acción de la organización, tanto hacia el interior como al exterior de la misma; • Incorporar la protección de datos personales y la privacidad a través del modelo de privacidad por o desde el diseño (*privacy by design*, PbD) como un aspecto crítico a considerar en el gobierno y gestión de la organización, y • Recibir retroalimentación sobre el cumplimiento en la materia y las necesidades planteadas para la toma de decisiones.	• Instruir sobre la necesidad de garantizar el cumplimiento como objetivo a conseguir en las operaciones diarias que implican el tratamiento de datos personales; • Proporcionar apoyo a quienes tienen que elaborar e implementar políticas para garantizar el cumplimiento en materia de protección de datos personales y privacidad, y • Supervisar el cumplimiento, con base en la retroalimentación recibida, tanto por lo que se refiere a cumplir con el objetivo de cumplimiento como a identificar brechas o desviaciones del objetivo.	• En el caso de cualquier proyecto nuevo, o incluso cuando se trate de un re-diseño de un sistema de información o un desarrollo tecnológico o revisión de prácticas de negocio, que dé lugar a tratamiento de datos personales de la propia organización, como responsable del tratamiento, o en nombre y por cuenta de otra organización, como encargado del tratamiento, implementar controles para identificar qué tratamientos de datos personales se llevan a cabo, considerando todos los aspectos relativos a dichos tratamientos (naturaleza de los datos personales, sensibilidad, etc.); cómo y para qué se obtienen y tratan los datos personales; qué datos son los necesarios (minimización del tratamiento) en atención a la finalidad o finalidades del tratamiento; si hay transferencias o remisiones, nacionales o internacionales, de datos personales; plazos de conservación de los datos personales; procedimientos para la destrucción de los datos personales; confidencialidad y seguridad de los datos personales; • Identificar y analizar riesgos derivados del tratamiento de los datos personales (tecnológicos, jurídicos u otros); • Medidas a adoptar para cumplir con el principio de responsabilidad o rendición de cuentas (arts. 6 y 14 de la LFPDPPP así como 47 y 48 del Reglamento) por el responsable y, en el caso del encargado del tratamiento, en virtud de las obligaciones contractuales con el responsable (art. 50 del Reglamento); • Alineación de dichas medidas/obligaciones con los principios de privacidad por diseño, y • Asignación de responsabilidad a quienes tratan datos personales en el desarrollo de sus funciones.
4 Ejecución	**5 Autoridades garante y reguladoras**	
• Recopilación de información, a través de los procedimientos establecidos, que sirva como retroalimentación para medir la efectividad de las medidas adoptadas e identificar incumplimientos o potenciales incumplimientos; • Necesidad de participar en acciones de formación y concientización continua para evitar puntos débiles que deriven en incumplimientos, y • Conocer su responsabilidad en el manejo de datos personales y las consecuencias de incumplir.	• Supervisa el cumplimiento; • Proporciona, en su caso, apoyo técnico para garantizar el cumplimiento por los responsables del tratamiento, y • Con sus acciones, interpreta la normatividad y difunde el conocimiento y cumplimiento en materia de protección de datos personales y privacidad. • Reconocer con algún instrumento a las empresas que cumplan eficientemente con la normativa.	

Para su implementación en la práctica, puede ser de gran utilidad, como referente, el documento *Operationalizing Privacy by Design: A guide to Implementing Strong Privacy Practices*[47]. Con base en dicho documento, es posible presentar la siguiente tabla que puede servir a su vez como metodología para implementación:

Principio	Acciones	Área / perfil
Proactivo, no Reactivo; ***Preventivo*** no Correctivo	**1.** Reafirmar el compromiso de la alta dirección con un programa de privacidad fuerte y proactivo. **2.** Asegurarse de que las acciones concretas, no sólo políticas, reflejan un compromiso con la privacidad. Monitorear periódicamente a través de un sistema de métricas. **3.** Desarrollar métodos sistemáticos para evaluar los riesgos de privacidad y seguridad y para corregir cualquier impacto negativo, mucho antes de que ocurran. **4.** Fomentar prácticas de privacidad demostrable compartidos por diversas comunidades de usuarios y grupos de interés, en una cultura de mejora continua.	• Alta dirección (por ejemplo, Junta Directiva, CEO, persona o departamento de datos personales –CPO-, CIO, COO, CSO, etc.).
Privacidad como la ***Configuración Predeterminada***	**1.** Adoptar una finalidad o finalidades tan reducida y específica como sea posible para la obtención de datos personales –comenzar con no recabar datos personales que no sean necesarios – minimización de los datos. **2.** Minimizar la obtención de datos desde el principio sólo a lo estrictamente necesario. **3.** Limitar el uso de información personal para los fines específicos para los que fue obtenida. **4.** Establecer límites tecnológicos, a través de políticas y procedimientos a los datos vinculados con información personal identificable.	• Ingenieros de software y desarrolladores. • Propietarios de aplicaciones y programas. • Propietarios de líneas de negocio y procesos.
Privacidad ***Incrustada*** en el Diseño	**1.** Hacer una evaluación de riesgos de privacidad como una parte integral de la fase de diseño de cualquier iniciativa, por ejemplo, en el diseño de la arquitectura técnica del sistema, prestando especial	• Propietarios de aplicaciones y programas. • Propietarios de líneas de negocio y procesos. • Ingenieros de software y

[47] Cuya autora es la Dra. Ann Cavoukian. Dicho documento está disponible en la dirección de Internet http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf [consultada el 6 de septiembre de 2014].

	atención a los posibles usos no previstos de los datos personales. **2.** Basar los metasistemas identidad en las "Leyes de la Identidad", destinadas a codificar un conjunto de principios fundamentales que son universalmente aceptados, debe cumplirse con una arquitectura identidad sostenible. **3.** Considerar la privacidad a lo largo del ciclo de vida de desarrollo de sistemas y procesos de ingeniería de la organización. Los diseñadores de sistemas deben ser alentados a innovar de manera responsable en el campo de la analítica avanzada. **4.** Insertar privacidad en enfoques regulatorios que pueden adoptar la forma de auto-regulación, leyes de privacidad sectoriales, normatividad general sobre protección de datos y privacidad y los marcos legislativos más generales, al proponer un enfoque basado en "la flexibilidad, el sentido común y el pragmatismo."	desarrolladores. • Autoridades reguladoras.
Funcionalidad Total – ***"Todos ganan"***, no "Si alguien gana, otro pierde"	**1.** Reconocer que intereses comerciales múltiples y legítimos deben coexistir. **2.** Entender, participar y colaborar - Practicar las 3Cs - comunicación, consulta y colaboración, para comprender mejor los intereses múltiples y, a veces, divergentes. **3.** Buscar soluciones y opciones innovadoras para lograr múltiples funcionalidades.	• Alta dirección. • Propietarios de aplicaciones y programas. • Propietarios de líneas de negocio y procesos. • Ingenieros de software y desarrolladores.
Seguridad Extremo-a-Extremo – ***Protección de Ciclo de Vida Completo***	**1.** Emplear el cifrado de forma predeterminada para mitigar los problemas de seguridad asociados a la pérdida, robo o eliminación de aparatos electrónicos tales como computadoras portátiles, tabletas, teléfonos inteligentes, USBs y otros medios externos. El estado por defecto de los datos, si son vulnerados, debe ser "ilegible". **2.** Implementar el cifrado correctamente e integrarlo con cuidado en los dispositivos y flujos de trabajo de forma automática y transparente. **3.** Garantizar la destrucción segura y la eliminación de la información personal al final de su ciclo de vida.	• Propietarios de aplicaciones y programas. • Propietarios de líneas de negocio y procesos. • Ingenieros de software y desarrolladores.
Visibilidad y ***Transparencia*** – Mantenerlo ***Abierto***	**1.** Poner a disposición del público y que sea bien conocida dentro de la organización la identidad y la información	• Alta dirección. • Ingenieros de software. • Desarrolladores de

(Comunicación con el cliente)	de contacto de la(s) persona(s) responsable(s) de la protección de datos personales y la seguridad. **2.** Implementar una política que exige que todos los documentos de acceso público *("publicfacing")* estén escritos en un "lenguaje claro" que sea fácilmente compresible para las personas cuya información está sujeta a las políticas y procedimientos. **3.** Hacer que la información sobre las políticas, procedimientos y controles relativos a la gestión de información personal esté a disposición de todos los individuos. **4.** Si se desea agregar un valor adicional sobre el cumplimiento también se podría: a) Considerar la publicación de los resúmenes de las evaluaciones de riesgos de privacidad (PIAs), evaluaciones de amenazas de riesgos (*"Threat Risk Assessment"*, TRA) y los resultados de auditorías de terceros independientes y b) Poner a disposición una lista de las bases de datos personales que mantiene la organización. **5.** Hacer del conocimiento del usuario sobre las metodologías y mejores prácticas sobre gestión de la información de la organización.	procedimientos y aplicaciones. • Arquitecto de sistemas.
Respeto por la Privacidad de los Usuarios – Mantener un Enfoque ***Centrado en el Usuario***	**1.** Ofrecer fuertes valores predeterminados de privacidad. **2.** Proporcionar un aviso de privacidad apropiado.	• Alta dirección. • Ingenieros de software y desarrolladores. • Propietarios de aplicaciones y programas. • Propietarios de líneas de negocio y procesos.

En vista de las consideraciones anteriores sobre el modelo de privacidad por diseño, es necesario, por lo tanto, que los responsables y encargados del tratamiento tengan un *roadmap* o plan de acción específico para la implementación de dicho modelo, pudiendo basarse el mismo conforme a los siguientes puntos de acción:

Roadmap o plan de acción específico para la implementación del modelo de *privacy by design*

1. Considerar la protección de datos y la privacidad en toda acción que implique el tratamiento de datos personales y a lo largo del ciclo de vida de los datos que, tanto al interior (por ejemplo, para recursos humanos) como al exterior (por ejemplo, de clientes), lleve a cabo una organización antes de iniciar el tratamiento.
2. Evaluar el impacto en la protección de datos que tendría dicho tratamiento, considerando todos los aspectos o factores tanto desde el punto de vista del riesgo como del cumplimiento de los principios y deberes aplicables al tratamiento.
3. Planificar las medidas a adoptar, en atención a las obligaciones que se tengan como responsable o encargado del tratamiento, y asignar responsabilidades.
4. Implementar las medidas de manera que cubran de extremo a extremo todos los ámbitos y áreas de la organización que impliquen o estén relacionados con el tratamiento de datos personales.
5. Evaluar la efectividad de las medidas adoptadas y mejorarlas de manera continua.

Como orientación final dirigida a quienes tratan datos personales, ya sea como responsables o encargados del tratamiento, el modelo de privacidad por diseño es una aproximación holística, ya que considera tanto el cumplimiento normativo como la adecuación de las prácticas de la organización, a la protección de datos personales, de manera que implica que el sujeto obligado deba adoptar medidas atendiendo a todos los aspectos que se plantean y que van desde la designación de una persona o departamento de datos personales durante todo el tratamiento y hasta la supresión segura de los datos personales.

El apoyo y compromiso de la alta dirección es fundamental, debiendo asegurarse que el compromiso con la protección de datos personales sea respetado por todas las personas de la organización, e incluso por los terceros con los que se mantengan relaciones jurídicas que impliquen o gobiernen el tratamiento de datos personales, y dicho compromiso debe concretarse en la elaboración de políticas u otros documentos, así como la adopción de medidas de diversa naturaleza (tecnológicas, administrativas, físicas, etc.) destinadas a alcanzar y mantener, de manera continua, un elevado nivel de protección de datos personales lo que permitirá generar confianza de las partes interesadas, evidenciar el compromiso con el cumplimiento y rendir cuentas en caso de que sea necesario, además de constituir una ventaja competitiva.

RESUMEN EJECUTIVO

1) **Antecedentes.** El presente estudio derivado del Proyecto "Privacy by Design para Fomentar la Figura del Encargado" (Procesos 2013) realizado a solicitud de la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI) con el respaldo del Prosoft 3.0 de la Secretaría de Economía, ha tenido como objetivo contar con elementos de análisis que sirvan para fomentar y coadyuvar al cumplimiento de la normatividad sobre protección de datos personales en el ámbito de las MIPYMES del sector de las Tecnologías de la Información (TI).

   El proyecto se suma a otros que la CANIETI ha promovido en materia de protección de datos personales, tales como los relacionados con autorregulación y la autogestión por parte de las empresas; y ahora se ha encauzado este que aborda el modelo canadiense de privacidad por diseño (Privacy by Design, PbD), con la finalidad de determinar su grado de adaptación en México y, en particular, por parte de MIPYMES del sector de TI. Todo esto, con el firme propósito de promover el desarrollo de una cultura empresarial de protección de datos personales.

   Para analizar el mencionado modelo este estudio se dividió en tres fases: **a)** La primera consistió en la investigación a nivel internacional del concepto de PbD, así como en un análisis práctico del mismo desde el punto de vista de la normatividad mexicana en protección de datos y de las implicaciones prácticas del concepto; **b)** La segunda fase comprendió la preparación y desarrollo de una entrevista con la precursora del PbD, la Dra. Ann Cavoukian, quien fuera Comisionada de la Oficina de Privacidad e Información de Ontario, Canadá, con el propósito de conocer de primera mano las características del modelo; y **c)** La tercera fase ha implicado analizar los beneficios e impactos de insertar el modelo PbD en el desarrollo e implementación de sistemas de información en las empresas, la implementación piloto del modelo de PbD en una empresa del Sector de TI, y la formulación de recomendaciones que sirvan a responsables y encargados del tratamiento para adoptar buenas prácticas a considerar en el diseño o re-diseño de un sistema de información y garantizar así el cumplimiento normativo en protección de datos personales. En esta sección se exponen a manera de Resumen Ejecutivo las conclusiones obtenidas en las mencionadas etapas del estudio.

2) **Definición de privacidad por diseño.** En primer lugar, cabe señalar que la traducción al español de privacy by design (PbD) puede dar lugar a diferentes términos, tales como privacidad por diseño, privacidad desde el diseño, privacidad en el diseño o privacidad mediante el diseño. Dichos términos deben entenderse como sinónimos.

El término privacidad por diseño fue desarrollado por la Dra. Ann Cavoukian y reconocido como estándar global de privacidad en octubre de 2010 a través de la Resolución sobre Privacidad por Diseño, adoptada durante la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad para dar respuesta a *"los efectos siempre crecientes y sistemáticos de las Tecnologías de la Información y las Comunicaciones, y de los sistemas de datos en red a gran escala".*

En la normatividad mexicana sobre protección de datos personales no hay una definición de este término, pudiendo encontrarse a modo de referencia una definición a nivel internacional en la Unión Europea, donde la Recomendación relativa a los preparativos para el despliegue de los sistemas de contador inteligente la define como la aplicación, teniendo en cuenta el estado de la técnica y el costo de dicha aplicación, tanto en el momento de la determinación de los medios de tratamiento como en el del tratamiento propiamente dicho, de las medidas y los procedimientos técnicos y de organización adecuados para que el tratamiento satisfaga los requisitos de la Directiva 95/46/CE y garantice la protección de los derechos del interesado.

La privacidad por diseño es una aproximación que, a través de los siete (7) principios fundamentales, tiene el propósito de especificar la protección que confieren los marcos regulatorios en materia de protección de datos personales y privacidad. Por lo tanto, se trata de garantizar la privacidad y la protección de datos personales en el diseño de prácticas de negocio o sistemas de información que implican, en cualquier caso, el uso de las Tecnologías de la Información y las Comunicaciones (TIC).

El concepto de privacidad por diseño está interrelacionado con otros conceptos, ya que a la misma se llega evaluando el impacto que tiene para la privacidad unas prácticas de negocio o un sistema de información, y estableciendo mecanismos de protección de datos personales por defecto a través de las mejores técnicas disponibles.

3) **Alcance de la privacidad por diseño.** La privacidad por diseño, se encuentra presente en todos los ámbitos de la actividad de una empresa u organización ya que hace referencia a los sistemas de información, los modelos y prácticas de negocio y el diseño físico e infraestructura en red.

   Además de asegurar la protección de datos personales, la privacidad por diseño es un elemento fundamental para conseguir otros objetivos, tales como impulsar el crecimiento económico, crear nuevos puestos de trabajo, fomentar la innovación, garantizar la privacidad, garantizar el derecho a la autodeterminación informativa y obtener una ventaja competitiva.

En cuanto a los sujetos obligados, los responsables y encargados del tratamiento, es necesario tomar en consideración que este último puede ofrecer productos o servicios que pueden ser utilizados por el responsable para el tratamiento de datos personales, de manera que debe adoptar las medidas para el cumplimiento de los principios y deberes previstos en la normatividad sobre protección de datos personales. En cualquier caso, la privacidad por diseño debe ser considerada tanto por el responsable como el encargado del tratamiento en cualquier acción que realicen y que implique un tratamiento de datos personales.

Sin perjuicio de los sujetos obligados, hay también otras figuras, tales como los fabricantes o desarrolladores de TI así como los proveedores de servicios de TI que, aunque no traten datos personales, deben considerar la privacidad por diseño ya que pondrán a disposición de responsables y encargados del tratamiento productos o servicios a través de los que se tratarán datos personales y que, por tanto, tienen que cumplir con principios y deberes en protección de datos personales.

Por último, la privacidad por diseño es también una cuestión a tomar en consideración por quienes tienen alguna responsabilidad en el cumplimiento de la normatividad sobre protección de datos personales, tales como desarrolladores de políticas públicas, legisladores, autoridades administrativas o judiciales competentes así como otras figuras.

4) **Ventajas de la privacidad por diseño.** Además de los objetivos que pueden alcanzarse con la privacidad por diseño, esta también permite obtener ventajas tales como facilitar el cumplimiento de la normatividad sobre protección de datos, ayudar a implementar tecnologías y buenas prácticas en materia de protección de datos personales, minimizar los riesgos derivados del tratamiento de datos personales y ahorrar costos. En definitiva, la privacidad por diseño genera confianza e impulsa la competitividad.

Por lo que se refiere al cumplimiento de los principios y deberes de protección de datos, la privacidad por diseño ayuda a restringir la obtención de datos personales al mínimo necesario (minimización del tratamiento = proporcionalidad); reducir o evitar tratamientos innecesarios o no deseados (licitud, finalidad y calidad); limitar los períodos de conservación (finalidad y calidad); hacer que el tratamiento sea respetuoso con la privacidad; conseguir que el tratamiento de datos personales sea transparente para los titulares de los datos personales; implementar medidas de seguridad (deber de seguridad), y ofrecer a los titulares de los datos personales herramientas para aumentar el control sobre el tratamiento (autodeterminación informativa).

5) **Los siete (7) principios fundamentales.** Los siete (7) principios fundamentales de la privacidad por diseño pueden ponerse en relación con los principios y deberes de la normatividad sobre protección de datos personales, de manera que: 1) Proactivo y preventivo está relacionado con la adopción de medidas en virtud del principio de responsabilidad; 2) Configuración predeterminada, privacidad en el diseño y funcionalidad (todos ganan) están relacionados con todos los principios y deberes; 3) Seguridad extremo-a-extremo está relacionado con el deber de medidas de seguridad; 4) Transparencia está relacionada con el principio de información y 5) Centrado en el usuario está relacionado con todos los principios y deberes, ya que se trata de garantizar la protección de datos personales.

6) **Referentes internacionales.** A nivel internacional, uno de los principales referentes es la Resolución sobre Privacidad por Diseño, adoptada durante la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que se celebró en Jerusalén, Israel, durante los día 27 a 29 de Octubre de 2010. Dicha resolución fue aprobada de manera unánime por las autoridades de protección de datos y privacidad como un componente esencial para la protección de la privacidad.

   En el ámbito de la Unión Europea hay varias normas que hacen referencia, bien sea de manera directa o indirecta, al modelo de privacidad por diseño, tales como la Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad; la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y la 2012/148/UE de la Comisión, de 9 de marzo, relativa a los preparativos para el despliegue inteligente de los sistemas de contador inteligente.

   Además, el futuro Reglamento general de protección de datos personales incluye un artículo específico que enuncia el modelo de privacidad desde el diseño y, en la práctica, obliga a los responsables del tratamiento a cumplir con el mismo.

   Otros referentes a nivel internacional son también las guías que diversas autoridades garantes o agencias de protección de datos personales han publicado.

   Por último, el Supervisor Europeo de Protección de Datos (SEPD), en virtud de su función consultiva, ha emitido diversos dictámenes en los que hace referencia o se centra en el modelo de privacidad por diseño y que sirven para el desarrollo de políticas públicas en la materia. Entre dichos dictámenes, cabe

destacar su Dictamen acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, en el que trata la cuestión relativa a cumplir con el modelo de privacidad por diseño de manera que el desarrollo tecnológico se haga conforme a los principios de la protección de datos personales.

En definitiva, la aplicación del modelo de privacidad por diseño trata de garantizar, desde la fase inicial de desarrollo de un sistema de información o planteamiento de un modelo de negocio y durante todo el ciclo de vida, la protección de datos personales a través de la aplicación de los principios y deberes exigibles.

7) **La normatividad mexicana y el modelo de privacidad por diseño.** Ni la LFPDPPP ni su Reglamento hacen referencia expresa a la privacidad por diseño, si bien es posible identificar algunas referencias indirectas. Entre estas, en la LFPDPPP, se encuentran el hecho de que el responsable del tratamiento tenga que velar por el cumplimiento de los principios de la protección de datos personales incluso cuando el tratamiento se haya encomendado al encargado del tratamiento. También el hecho de tener que resguardar los datos personales de manera que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) sin dilación, implica que se deban adoptar medidas en cuanto al diseño de la base de datos o sistema de información en el que se traten.

   En el caso del Reglamento de la LFPDPPP, los artículos 47 y 48 relativos al principio de responsabilidad y a las medidas para cumplir con el mismo, suponen que tanto el responsable como el encargado del tratamiento tengan que adoptar medidas para garantizar la protección de datos personales, pudiendo ser una de dichas medidas la privacidad por diseño.

   Otra normatividad a tomar en consideración puede ser, por una parte, los Parámetros de autorregulación vinculante, ya que entre los contenidos complementarios podría incluirse la adopción de medidas en virtud del modelo de privacidad por diseño y, por otra parte, la Ley Federal de Telecomunicaciones, puesto que entre las medidas técnicas a adoptar por una operadora de telecomunicaciones para la conservación de datos personales, deben tomar en consideración la privacidad por diseño en sus bases de datos a efectos de garantizar la protección de datos personales.

   En definitiva, la privacidad por diseño implica adoptar medidas para garantizar los principios de la protección de datos, deberes (seguridad y confidencialidad), así como derechos ARCO desde el inicio, incluso antes de tratar datos personales.

8) **Entrevista con la Dra. Ann Cavoukian: creadora del concepto Privacy by Design.** Una parte importante de este trabajo fue lograr una entrevista con la precursora del PbD, la Dra. Ann Cavoukian, quien fuera Comisionada de la Oficina de privacidad e información de Ontario, Canadá de 1997 al 2014. Nacida en 1952 en El Cairo, Egipto; es hija de padres armenios emigró a Toronto, Canadá en 1958, lugar donde estudió un BA en la Universidad de York. Cuenta con maestría y doctorado en sicología por la Universidad de Toronto y se ha especializado en criminología y derecho. La Dra. Cavoukian ha recibido múltiples galardones y es reconocida como una de las principales expertas de privacidad en el mundo, por lo que empresas importantes de Estados Unidos, Canadá y Europa le solicitan orientación sobre herramientas y política en materia de protección de datos personales. Actualmente la Dra. Cavoukian es Directora Ejecutiva del Instituto de Privacidad y Big Data (The Privacy and Big Data Institute) en la Universidad de Ryerson.

   El eje central de la entrevista fue obtener elementos emanados de la propia autora del concepto de PbD que sirvan como referentes a las MIPYMES del sector de las Tecnologías de la Información (TI) de México para que lo puedan aprovechar o replicar en su caso y se fomente el cumplimiento de la normatividad sobre protección de datos personales.

   Es de reconocer que cuando fue contactada la Dra. Cavoukian, tanto ella como su equipo de colaboradores mostraron toda la disposición de cooperar en la absolución del cuestionario que elaboró el consultor y le fue enviado de manera oficial por la titular de la Dirección de Economía Digital a través del oficio (oficial letter 410.3.14/0707).

   De la entrevista se destaca lo siguiente:

   - La privacidad es acerca del control individual – mantener control personal sobre la recolección, uso y divulgación de nuestros datos personales. El derecho de los individuos a ejercer control sobre sus datos personales apoya libertades fundamentales y los protege de la tiranía.
   - La ex comisionada Ann Cavoukian desarrolló Privacidad por Diseño a mediados de los 90's para proactivamente proteger los intereses de la privacidad previniendo que el daño a la privacidad aumente. Los principios de prácticas legítimas de la información (FIPPs por sus siglas en inglés) no solamente fueron directamente incluidos en el diseño de tecnologías de la información y de los procesos operacionales, también fueron superados a través de principios tales como de suma-positiva, no de suma-cero y privacidad como configuración por defecto.
   - Los principios de PbD se basaron en y extendieron los FIPPs tradicionales que actualmente sirven como base de las leyes de privacidad, políticas y

prácticas. Una manera para los ingenieros y abogados de concebir la PbD es pensar en ellos como FIPPs aplicadas con firmeza, con énfasis adicional en ser proactivo, sistemático y orientado a resultados.

- Los esfuerzos para "construir privacidad en el código" provee seguridad creíble en el compromiso de una entidad en cuanto a las promesas de privacidad, mayor evidencia de cumplimiento regulatorio y para que otros emulen las mejores prácticas.
- El Comité Técnico para Ingenieros de Programación Privacidad por Diseño OASIS (PbD-SE por sus siglas en inglés) ha desarrollado un borrador de especificaciones para ayudar a documentar las decisiones de privacidad de ingeniería de programación que sean consistentes con la PbD y los FIPPs.
- Los principios de PbD son universales por naturaleza y pueden ser aplicados por organizaciones de cualquier tamaño, en cualquier lugar y en cualquier momento.
- Los principios de PbD tienen aplicación universal y pueden aplicarse igualmente por desarrolladores de aplicaciones así como por corporaciones multinacionales más grandes o por entidades gubernamentales.
- Aplicar sistemáticamente los principios de manera proactiva y creativa lleva generalmente a prácticas de gestión de datos mejores y más eficientes. Menor filtración de datos, mejora en la seguridad del cliente, confianza y menor rotación así como el reconocimiento del liderazgo de la privacidad son beneficios típicos reportados por aquellos que adoptaron PbD.
- A la fecha no se tiene evidencia de que, adoptar las prácticas de privacidad con firmeza, impida la innovación o limite el éxito de la mayoría de los modelos de negocios. De hecho, la evidencia a la fecha indica que el verdadero obstáculo es el no apreciar el potencial de la privacidad y no adoptar la protección de privacidad de maneras creativas y de suma-positiva.
- Los proveedores de servicios sociales, móviles y en la nube diseñan y operan plataformas de creciente localización, complejidad y volúmenes de datos personales. Sus actividades deben ser más entendibles y deben rendir cuentas a sus usuarios.
- Todos somos responsables de la privacidad en una organización, sin embargo tareas en particular recaen en el Oficial Jefe de Privacidad, el Consejo de Directores y el Equipo Ejecutivo en general. Todas las organizaciones deben nombrar una persona de contacto para privacidad.
- PbD reduce los riesgos de un error humano.
- PbD provee evidencia de cumplimiento de debida diligencia de privacidad (queja o filtración).

- Cuatro de los principios de PbD promueven la rendición de cuentas (a los consumidores, reguladores, socios de negocios, accionistas, miembros del equipo
- PbD incluye "privacidad por defecto." Privacidad (Configuración) por defecto es el principio #2, el cual enfatiza minimizar datos y otros límites en la obtención, uso y divulgación de datos personales, incluyendo configuraciones firmes de privacidad por defecto.
- En octubre de 2010, PbD fue reconocida como una norma internacional en una resolución emblemática por la Conferencia Internacional de Protección de Datos y Comisionados de Privacidad en Jerusalén. Desde entonces, los 7 Principios Básicos de PbD han sido traducidos a más de 37 idiomas oficiales.
- Las propuestas de reformas regulatorias en EEUU y UE han hecho referencia a los principios de Privacidad por Diseño.
- Cursos de Ingeniería de Privacidad por Diseño se ofrecen en las principales universidades de EEUU y la UE.
- El Comité Técnico de Normas Internacionales (OASIS PbD-SE por sus siglas en inglés) aprobó un borrador de especificaciones para documentar PbD en software de ingeniería.
- Más de 300 personas y organizaciones han sido nombrados como Embajadores de PbD.
- El trabajo continuará mundialmente para hacer operativos los Principios PbD y establecer los estándares para evaluar el cumplimiento de esos principios en varios ámbitos.
- Nunca debemos perder de vista el hecho de que la privacidad moderna es un derecho humano, y no debemos considerarla como un obstáculo, inconveniente o compararla como un "daño" simple a ser mitigado. La implementación del Modelo PbD debe enfatizar el control individual y la rendición de cuentas organizacional en un balance armonioso.

9) **Implementación piloto en una empresa de TI**. Como antes se señaló una importante fase del proyecto consiste en la realización de un análisis -desde el punto de vista técnico- sobre los beneficios e impactos de insertar el modelo PbD en el desarrollo e implementación de sistemas de información en las empresas. Para tal efecto, se llevó a cabo la implementación piloto del modelo de PbD en una empresa del Sector de TI a fin de estar en posibilidades de emitir las recomendaciones que sirvan a responsables y encargados del tratamiento para adoptar buenas prácticas a considerar en el diseño o re-diseño de un sistema de información y garantizar así el cumplimiento normativo

en protección de datos personales. Concretamente se trabajó en una empresa cuyo objeto social principal es la proveeduría de soluciones informáticas.

10) **Alcance de las recomendaciones**. Las recomendaciones emanadas del estudio teórico y de la implementación piloto, en materia del modelo de privacidad por diseño (*privacy by design*, PbD), se dirigen tanto a la Secretaría de Economía, en su papel de autoridad reguladora, como a los responsables y encargados del tratamiento, quienes están sujetos al cumplimiento de la normatividad sobre protección de datos personales. El papel que desempeñe la Secretaría de Economía, como autoridad reguladora, con respecto al modelo de privacidad por diseño, es fundamental, ya que de ello puede depender que dicho modelo se materialice en la realidad, al facilitar a responsables y encargados del tratamiento orientación sobre el mismo de manera que puedan aprovecharse las ventajas que ofrece y ser también una marca que permita distinguir claramente el desarrollo de tecnología y servicios que cumplan con protección de datos personales y privacidad. Al mismo tiempo, los responsables y encargados del tratamiento pueden encontrar en el modelo de privacidad por diseño un instrumento adecuada tanto para implementar medidas que favorezcan el cumplimiento de la normatividad sobre protección de datos personales, como una filosofía que permita implementar buenas prácticas en todas las áreas de la organización, así como divulgar el conocimiento de este derecho fundamental entre todas las personas implicadas en el tratamiento de datos personales en las operaciones diarias.

11) **Recomendaciones a la Secretaría de Economía.** La implementación y, en su caso, cumplimiento del modelo de privacidad por o desde el diseño no es sólo una cuestión que incumba a los responsables y encargados del tratamiento, sino que requiere también de la adopción de medidas por las autoridades competentes que, en materia de protección de datos personales en posesión de los particulares, son tanto el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), en su papel de autoridad garante, como la Secretaría de Economía, en el desarrollo de sus funciones como autoridad reguladora (Artículo 43 de la LFPDPPP) que son clave para apoyar en la práctica la adopción e implementación del modelo de privacidad por o desde el diseño en México. En concreto, a la vista de la evolución del modelo de privacidad por diseño desde que fue acuñado en los años 90 por la Dra. Ann Cavoukian, el reconocimiento de dicho modelo a nivel internacional, sería recomendable que la Secretaría de Economía, como autoridad reguladora y con atribuciones en materia de protección de datos personales en el ámbito comercial, pudiera:

- Desempeñar una labor de concientización dirigida a los responsables y encargados del tratamiento, así como en su caso a otros sujetos tanto del sector privado como del sector público involucrados en promover el derecho fundamental a la protección de datos personales, con la finalidad de que el

modelo de privacidad por o desde el diseño sea adoptado e implementado por los responsables y encargados del tratamiento;

- Divulgar información sobre el modelo de privacidad por diseño como un instrumento adecuado que permita elaborar un plan de acción tomando en consideración la protección de datos personales y la privacidad desde la fase más temprana de diseño y desarrollo de la arquitectura de los sistemas de tecnologías de la información y prácticas de negocio;
- Fomentar la adopción e implementación del modelo de privacidad por diseño como una buena práctica en el ámbito comercial, siendo éste en el que se produce una gran parte de avances tecnológicos que requieren ser desarrollados conforme a dicho principio para garantizar así la protección de datos personales y la privacidad;
- Diseñar e instrumentar políticas públicas cuya finalidad sea el conocimiento por los responsables y encargados del tratamiento, en el ámbito comercial, de las obligaciones que tienen a la hora de tratar datos personales, incluyendo la conveniencia de implementar el modelo de privacidad por diseño;
- Realizar eventos con la participación de todos los actores involucrados en materia de protección de datos personales, con la finalidad de dar a conocer el modelo de privacidad por diseño, sus beneficios e implicaciones para el desarrollo de servicios y tecnologías que cumplan con la protección de datos personales, lo que a su vez puede convertirse en una marca que sirva para generar confianza de los usuarios;
- Apoyar la elaboración de estudios y monitoreo de avances que se produzcan a nivel internacional sobre el modelo de privacidad por diseño, de manera que México aproveche la experiencia acumulada a nivel internacional y la pueda transformar en buenas prácticas de las que se beneficien los responsables y encargados del tratamiento que tienen que cumplir con la normatividad sobre protección de datos personales;
- Apoyar, en el ámbito de sus competencias, la adopción de medidas que tengan por objeto la adopción e implementación del modelo de privacidad por diseño a nivel nacional, de manera que pueda plasmarse en políticas públicas, lineamientos u otros instrumentos que sean vinculantes para responsables y encargados del tratamiento;
- Divulgar, a través de los instrumentos y/o foros o eventos oportunos, la interrelación del modelo de privacidad por diseño con los principios de la protección de datos personales, y en particular, con el principio de responsabilidad o rendición de cuentas, así como el papel que puede desempeñar al respecto la persona o departamento de datos personales;
- Fomentar la inclusión del modelo de privacidad por diseño en esquemas de autorregulación en materia de protección de datos personales,

aprovechando a tal fin los Parámetros de Autorregulación en materia de Protección de Datos Personales;

- Educar a responsables y encargados del tratamiento sobre los beneficios que implica el modelo de privacidad por diseño, tanto por lo que se refiere a garantizar el cumplimiento de la normatividad sobre protección de datos personales, lo que permite reducir el riesgo derivado del tratamiento y uso de datos personales, así como que se trata de una buena práctica de negocio, que debe regir todos los tratamientos de datos personales, y
- Actuar en coadyuvancia con el IFAI buscando áreas de oportunidad en las que sus acciones puedan tener la mayor repercusión e impacto posibles, con la finalidad de que la implementación de modelos como el de privacidad por diseño u otras acciones redunden en beneficio tanto de los responsables y encargados del tratamiento como de las personas cuyos datos personales son tratados, lo que a su vez permitirá a México ser un ejemplo a seguir por sus socios comerciales y otros países.

12) **Recomendaciones Dirigidas a responsables y encargados del tratamiento.** En el caso de los responsables y encargados del tratamiento, quienes tienen que adoptar medidas para cumplir con las obligaciones que les son exigibles conforme a la LFPDPPP, su Reglamento y demás normatividad aplicable, es necesario que éstos puedan contar con una regulación clara, que a su vez pueda ser complementada por la autorregulación. En concreto, el modelo de privacidad por o desde el diseño, permitirá a los responsables y encargados del tratamiento, cumplir desde el inicio con la normatividad y requisitos en materia de protección de datos personales, lo que supone minimizar el riesgo de sanción; otros riesgos, como por ejemplo la pérdida de confianza por parte de potenciales clientes, clientes o accionistas, autoridades administrativas y judiciales competentes; así como embeber o incorporar los principios de protección de datos personales y privacidad en todas las áreas y acciones de la organización. Las recomendaciones se resumen de la forma siguiente:

   - A la hora de implementar o incorporar el modelo de privacidad por diseño, la organización tiene que ser activa, partiendo del hecho de que dicho principio está estrechamente interrelacionado con el cumplimiento de las obligaciones que tiene la misma en el cumplimiento de la normatividad sobre protección de datos personales ya sea como responsable o encargado del tratamiento.
   - Además de conocer el significado y alcance del modelo de privacidad por diseño, pudiendo desempeñar la persona o departamento de datos personales un papel relevante al respecto, cualquier responsable o encargado del tratamiento que trate datos personales, debe contar con un *roadmap* o plan de acción a través de la que se tome en consideración el

modelo de privacidad por diseño a la hora de adoptar medidas para cumplir con la normatividad sobre protección de datos personales.

- Una propuesta de *roadmap* en que el responsable o encargado del tratamiento tenga una posición proactiva al cumplimiento, lo que implica aportar recursos necesarios, cualquiera que sea su naturaleza (materiales, humanos, financieros, etc.), considerando el cumplimiento de la protección de datos personales como una ventaja competitiva.
- Para su aplicación en la práctica, el modelo de privacidad por diseño puede resumirse de la siguiente forma:

Modelo de privacidad por o desde el diseño (privacy by design, PbD)		
Aplica a	Datos personales:	Todos los tipos de datos personales
	Organizaciones:	Cualquier tipo de organización
	Ámbitos:	• Sistemas de tecnologías de la información • Prácticas de negocio responsables (compliance) • Diseño físico e infraestructura en red
Atiende a	Sensibilidad de los datos, considerando su naturaleza	
Objetivos	3) Garantizar la privacidad, y 4) Ser una ventaja competitiva sostenible.	
Principios	8) ***Proactivo***, no Reactivo; ***Preventivo*** no Correctivo 9) Privacidad como la ***Configuración Predeterminada*** 10) Privacidad ***Incrustada*** en el Diseño 11) Funcionalidad Total – ***"Todos ganan"***, no "Si alguien gana, otro pierde" 12) Seguridad Extremo-a-Extremo – ***Protección de Ciclo de Vida Completo*** 13) ***Visibilidad*** y ***Transparencia*** – Mantenerlo ***Abierto*** 14) ***Respeto*** por la Privacidad de los Usuarios – Mantener un Enfoque ***Centrado en el Usuario***	

- Con carácter general, las medidas a adoptar y adoptadas en virtud del modelo de privacidad por o desde el diseño, conforme a la responsabilidad de cada área de la organización, deben dar lugar a su vez a conseguir los siguientes objetivos:
  a) En relación con el modelo de privacidad por diseño, por cada una de las áreas de la organización, así como en su caso otras partes interesadas, tales como la autoridad garante y las autoridades reguladoras, es posible presentar la siguiente propuesta de *roadmap* o plan de acción, dirigida a responsables y encargados del tratamiento para que les sirva al momento de adoptar buenas prácticas a considerar en el diseño o re-diseño de un sistema de información y garantizar así el cumplimiento normativo en protección de datos personales, es la que se incluye a continuación:

b) Para su implementación en la práctica, puede ser de gran utilidad, como referente, el documento *Operationalizing Privacy by Design: A guide to Implementing Strong Privacy Practices* cuya autora es la Dra. Ann Cavoukian. Con base en dicho documento, en la **Parte II** del **Entregable** 3 de este Proyecto se propone una tabla que puede servir como metodología para implementación.

c) Es necesario que los responsables y encargados del tratamiento tengan *roadmap* o plan de acción específico para la implementación del modelo de *privacy by design*.

❖ Como orientación final dirigida a quienes tratan datos personales, ya sea como responsables o encargados del tratamiento, el modelo de privacidad por diseño es una aproximación holística, ya que considera tanto el cumplimiento normativo como la adecuación de las prácticas de la organización, a la protección de datos personales, de manera que implica que el sujeto obligado deba adoptar medidas atendiendo a todos los aspectos que se plantean y que van desde la designación de una persona o departamento de datos personales hasta la supresión segura de los datos personales.

13) Beneficios e impactos de la inserción del Modelo de PbD en las empresas de TI. Insertar el modelo de privacidad por o desde el diseño (*privacy by design*, PbD) en el desarrollo e implementación de sistemas de información en organizaciones, modelos o prácticas de negocio y en el diseño físico e infraestructura, tiene importantes beneficios e impactos positivos Derivado del presente estudio, es posible presentar a continuación varios puntos relevantes:

- **El concepto de privacidad por diseño es amplio pero suficientemente preciso:** Es necesario recordar que el concepto sigue vigente dos décadas después de que fuera acuñado a mediados de los años 90 por la Dra. Ann Cavoukian, y que el mismo abarca diferentes casos (desarrollo e implementación de sistemas de información en organizaciones, modelos o prácticas de negocio y en el diseño físico e infraestructura), y aplica a cualquier tipo de organización, con independencia de su tamaño y área de actividad, así como *"en cualquier lugar y en cualquier momento"*. Por lo tanto, es necesario pensar en el principio también como una filosofía, en cuanto a que a través del mismo es posible concientizar a las organizaciones, ya sean responsables o encargados del tratamiento, de la necesidad de adoptar e implementar medidas para cumplir con los principios y deberes previstos en la normatividad sobre protección de datos personales.

- **El modelo de privacidad por diseño ha sido reconocido a nivel internacional tanto por las autoridades de protección de datos personales como por la normativa:** Siendo buena muestra de ello el hecho de que las autoridades de protección de datos personales y privacidad a través de la Resolución sobre Privacidad por Diseño, adoptada durante la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en 2010; así como por otras varias autoridades de protección de datos personales alrededor del mundo, como por ejemplo, Reino Unido, Alemania y Australia o la Comisión Federal de Comercio (*Federal Trade Commission*, FTC) de los Estados Unidos de América, además del Supervisor Europeo de Protección de Datos (SEPD). En el caso de la Unión Europea, pueden encontrarse referencias en la Recomendación 2012/148/UE relativa a los preparativos para el despliegue inteligente de los sistemas de contador inteligente y en el Reglamento general de protección de datos se incluye un artículo que hace referencia de manera específica al modelo de privacidad por diseño.

- **En México no se encuentran referencias al modelo de privacidad por diseño:** Ni la normatividad sobre protección de datos personales, la LFPDPPP y su Reglamento, ni las autoridades competentes en la materia, principalmente el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y las autoridades reguladoras, se han referido al modelo de privacidad por diseño, siendo este estudio promovido por la Secretaría de Economía el primero en sus formas teórica como práctica.

- **No hay métricas sobre el modelo de privacidad por diseño:** Analizar el impacto en la práctica del modelo de privacidad por diseño resulta complejo. De las respuestas de la Dra. Ann Cavoukian a la entrevista hecha durante este proyecto, cabe resaltar que en relación con este modelo *"[a]plicar sistemáticamente los principios de manera proactiva y creativa lleva generalmente a prácticas de gestión de datos mejores y más eficientes. Menor filtración de datos, mejora en la seguridad del cliente, confianza y menor rotación así como el reconocimiento del liderazgo de la privacidad son beneficios típicos reportados por aquellos que adoptaron PbD."* Esto significa que deban, en su caso, desarrollarse métricas para medir los niveles de cumplimiento y, en su caso, incumplimiento de los principios y, también, de la normatividad aplicable.

- **El modelo de privacidad por diseño todavía está en evolución:** Entre las razones para no encontrar métricas concretas, debe atenderse a que una de las respuestas dadas por la Dra. Ann Cavoukian en la entrevista fue *"El trabajo continuará mundialmente para hacer operativos los Principios PbD y establecer los estándares para evaluar el cumplimiento de esos principios en varios ámbitos."* La respuesta representa una oportunidad

para México, que podría adoptar medidas para adoptar los principios de privacidad por diseño o, en su caso, desarrollar métricas específicas conforme a los principios que estime oportunos.

- **El modelo de privacidad por diseño es desconocido en México:** El programa piloto llevado a cabo como parte del presente proyecto ha supuesto explicar y concientizar a la empresa que amablemente aceptó participar, siendo relevante el hecho de que la misma tenga un nivel de cumplimiento de la normatividad sobre protección de datos personales, si bien el modelo de privacidad por diseño resulta novedoso para la misma siendo una cuestión sobre la que la empresa desea trabajar para aumentar las medidas que ya ha adoptado hasta el presente.

- **Es necesario dar visibilidad a los análisis y materiales de la Secretaría de Economía:** A pesar de que durante los últimos años la Secretaría de Economía viene desempeñando una importante labor, atendiendo específicamente a promover la figura del encargado del tratamiento, los resultados pueden no estar siendo aprovechados por los responsables y encargados del tratamiento.

- **A la hora de ponerlo en práctica, el modelo de privacidad por diseño debe considerarse a la luz de los principios y deberes de la LFPDPPP y su Reglamento:** Lo que supone que deba atenderse tanto a los principios y deberes, especialmente por lo que se refiere a las medidas a adoptar en virtud del principio de responsabilidad y sobre el resto de principios, como otras obligaciones previstas en la normatividad, tales como la designación de una persona o departamento de datos personales, que puede ser además la figura clave para velar o apoyar que se implemente este modelo de privacidad por diseño, siendo además un aspecto o cuestión sobre la que se requiere el impulso por parte de la Secretaría de Economía, otras autoridades garantes y, en última instancia, el IFAI.

14) **Importancia del compromiso corporativo**. El apoyo y compromiso de la alta dirección es fundamental, debiendo asegurarse que el compromiso con la protección de datos personales sea respetado por todas las personas de la organización, e incluso por los terceros con los que se mantengan relaciones jurídicas que impliquen o gobiernen el tratamiento de datos personales, y dicho compromiso debe concretarse en la elaboración de políticas u otros documentos, así como la adopción de medidas de diversa naturaleza (tecnológicas, administrativas, físicas, etc.) destinadas a alcanzar y mantener, de manera continua, un elevado nivel de protección de datos personales lo que permitirá generar confianza de las partes interesadas, evidenciar el compromiso con el cumplimiento y rendir cuentas en caso de que sea necesario, además de constituir una ventaja competitiva.

15) **Importancia de la promoción de una cultura empresarial a favor de la privacidad**. La promoción del cumplimiento de la normatividad es muy importante, para lo cual puede verse la Encuesta Nacional de Protección de Datos Personales 2012, elaborada por el IFAI, y conforme a la cual se puede concluir que la percepción de la mayoría de las empresas que participaron en la misma es que la mayoría (76%) *"considera que la LFPDPPP tiene muchísima o mucha utilidad"*. Ahora bien, es necesario tomar en consideración que la realidad es que el *"84% de las empresas desconoce las obligaciones derivadas de la entrada en vigor de la LFPDPPP."* Es importante que las empresas también se vean reconocidas con algún instrumento por parte del IFAI cuando cumplan eficientemente con la normativa, lo cual fomentará el interés y participación de las empresas en favor de la privacidad.

Bibliografía básica

— Bar Council of England and Wales; Response of the Bar Council of England and Wales to the European Commission´s consultation on its comprehensive approach to Personal data protection in the European Union, January 2011; disponible el 8 de febrero de 2014 en el vínculo electrónico: http://www.barcouncil.org.uk/media/53885/bar_council_of_ew_lrc_final_response_to_eu_consultation_on_data_protection_19-1-11.pdf

— Brian Nougrères, Ana; La protección inteligente de los datos personales: *Privacy by design* (PbD), Revista Internacional de Protección de Datos Personales, No. 1 Julio – Diciembre de 2012; disponible el 5 de septiembre de 2014 en el vínculo electrónico: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf

— Cavoukian, Ann; Privacy by Design: Achieving Consumer Trust and Freedom in the Information Age, Management Ethics, Fall/Winter 2010; disponible el 8 de febrero de 2014 en el vínculo electronico: http://www.ethicscentre.ca/en/files/speeches/management_ethics_fw10_dh.pdf

A Regulator´s Perspective on Privacy by Design; disponible el 9 de febrero de 2014 en el vínculo eletrónico: http://webcache.googleusercontent.com/search?q=cache:SCKv22ATtIQJ:www.futureofprivacy.org/wp-content/uploads/A-Regulators-Perspective-on-Privacy-by-Design.doc+&cd=15&hl=en&ct=clnk&gl=es

— Center for Democracy & Technology, The Role of Privacy by Design in Protecting Consumer, January 28, 2010; disponible el 8 de febrero de 2014 en el vínculo electrónico: https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy

— Davies, Simon; Why Privacy by Design is the next crucial step for privacy protection, November 2010; disponible el 8 de febrero 2014 en el vínculo electrónico: http://www.i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf

— European Union Agency for Network and Information Security; Privacy, Accountability and Trust - Challenges and Opportunities, February 18, 2011; disponible el 9 de febrero de 2014 en el vínculo electrónico:
http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study/at_download/fullReport

— Ernst and Young; *Asuntos relevantes sobre Protección de Datos Personales para 2011, Los retos que enfrentan los programas de Privacidad de la Información en un mundo sin fronteras*, Marzo de 2011; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://www.ey.com/Publication/vwLUAssets/Folleto_Asuntos_relevantes_sobre_Proteccion_de_Datos_Personales_para_2011/$FILE/Asuntos_Relv_Protec_datos.pdf

— European Data Protection Supervisor; EDPS opinion on privacy in the digital age: "Privacy by Design" as a key tool to ensure citizens´ trust in ICTs, Press Release, 22 March 2010; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://europa.eu/rapid/press-release_EDPS-10-6_en.htm

Dictamen del Supervisor Europeo de Protección de Datos acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, Diario Oficial de la Unión Europea, serie C número 280, de 16 de octubre de 2010; disponible el 8 de febrero de 2014 en el vínculo electrónico:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_ES.pdf

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union", 14 January 2011; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(2)_15th_rt_2011.pdf

Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union; disponible el 14 de febrero de 2014 en el vínculo electrónico:
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf

Introductory remarks on Presentantion of European Privacy Seals, 13 November 2008; disponible el 14 de febrero de 2014 en el vínculo electrónico: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2008/08-11-13_Speech_Europrise_EN.pdf

Data Protection in Schleswig-Holstein, in Europe and in a Global Information Society, 14 July 2008; disponible el 14 de febrero de 2014 en el vínculo electrónico:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2008/08-07-14_Kiel_info_society_EN.pdf

— Federal Trade Commission; Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, March 2012; disponible el 8 de febrero de 2014 en el vínculo electrónico: http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

— GSMA Association; Directrices para el diseño de privacidad en el desarrollo de aplicaciones, Junio 2012; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://www.gsma.com/latinamerica/wp-content/uploads/2012/07/Privacy-Guidelines-Spanish-booklet-20120613-LR.pdf

— Gürses, Seda, Troncoso, Carmela, y Diaz, Claudia; Engineering Privacy by Design; disponible el 8 de febrero de 2014 en el vínculo electrónico: http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf

— Information Commissioner´s Office of the United Kingdom; Privacy by Design, November 2008; disponible el 8 de febrero de 2014 en el vínculo electrónico http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PRIVACY_BY_DESIGN_REPORT_V2.ashx

Privacy by Design Report Recommendations: ICO Implementation Plan, 26 November 2008; disponible el 8 de febrero de 2014 en el vínculo electrónico: http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PBD_ICO_IMPLEMENTATION_PLAN.ashx

— Information and Privacy Commissioner of Ontario, Canada; Privacy by Design, Strong Privacy Protection – Now, and Well into the Future, A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners, 2011; disponible el 8 de febrero de 2014 en el vínculo electrónico: http://www.ipc.on.ca/images/Resources/PbDReport.pdf

— International Chamber of Commerce (ICC); ICC Comments on EU General Data Protection Regulation Issues, 15 January 2013; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://www.iccwbo.org/Data/Policies/2013/ICC-comments-EU-General-DP-Reg-Issues/

— International Peace Research Institute; Recommendation Report: Situating Privacy and Data Protection in a Moving European Security Continuum; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://www.vub.ac.be/LSTS/pub/Dehert/456.pdf

— Krebs, David, “Privacy by Design”: Nice-to-have or a Necessary Principle of Data Protection Law?, Jipitec, 2013; disponible el 8 de febrero de 2014 en el vínculo electrónico http://www.jipitec.eu/issues/jipitec-4-1-2013/jipitec4krebs/jipitec-4-1-2013-2-krebs.pdf

— Langheinrich, Marc; Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems; disponible el 9 de febrero de 2014 en el vínculo electrónico:
http://cs.gmu.edu/~jpsousa/classes/699/papers/privacy%20Langheinrich.pdf

— Métayer, Daniel Le; Privacy by Design: a Formal Framework for the Analysis of Architectural Choices (Extended Version), Inria Informatics Mathematics, Research Report Nº 8229, February 2013; disponible el 9 de febrero de 2014 en el vínculo electrónico:
http://hal.archives-ouvertes.fr/docs/00/78/85/84/PDF/RR-8229.pdf

— Microsoft, Privacy by Design at Microsoft, March 2012; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/privacy_by_design.pdf

— Ministry of Justice of the United Kingdom; Summary of Responses, Call for Evidence on Proposed EU Data Protection Legislative Framework, 28 June 2012; disponible el 8 de febrero de 2014 en el vínculo electrónico:
https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/summary-responses-proposed-data-protection-legislation.pdf

— Robinson, Neil, Graux, Hans, Botterman, Maarten y Valeri, Lorenzo; Review of EU Data Protection Directive: Technical Report,, 2009; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf

Review of EU Data Protection Directive: Summary, Prepared for the Information Commissioner´s Office, May 2009; disponible el 8 de febrero de 2014 en el vínculo electrónico:http://ico.org.uk/about_us/research/~/media/documents/library/Data_Protection/Detailed_specialist_guides/REVIEW_OF_EU_DP_DIRECTIVE_SUMMARY.ashx

— Rost, Martin y Bock, Kirsten; Privacy by Design and the New Protection Goals; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://maroki.org/pub/privacy/BockRost_PbD_DPG_en_v1f.pdf

— Rubinstein, Ira y Good, Nathan; Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, August 11, 2012; disponible el 9 de febrero de 2014 en el vínculo electrónico:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128146

— Santucci, Gerald; Privacy in the Digital Economy: Requiem or Renaissance? An essay on the future of privacy, The Privacy Surgeon, September 2013; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://www.privacysurgeon.org/blog/wp-content/uploads/2013/09/Privacy-in-the-Digital-Economy-final.pdf

— Schwartz, Paul M.; The E.U.-US Privacy Collision: A Turn to Institutions and Procedures; 10 February 2012; disponible el 8 de febrero de 2014 en el vínculo electrónico:
http://www.harvardlawreview.org/symposium/papers2012/schwartz.pdf

Proyecto: "Privacy by design para fomentar la figura del encargado [Procesos 2013]"

— 3ª entrega: Entrega Final –

Elaborado por:

GEV Asesores Internacionales, S.C.

Para:

México, D.F., Septiembre 15 de 2014