

Alineación a la LFPDPPP
Technology Risk Services

Julio 7, 2011

Mayra Rivera Marchesini, Gerente ERS
Technology Risk Services



Contenido

1.- Introducción

- ¿Quién tiene que cumplir con la LFPDPPP?
- Principios de Protección de Datos Personales
- Nuestra visión general de la LFPDPPP
- Principios de Privacidad Generalmente Aceptados
- Beneficios de buenos controles de privacidad
- Roadmap

2.- Aviso de Privacidad

- Modalidades de aviso de privacidad
- Medidas compensatorias

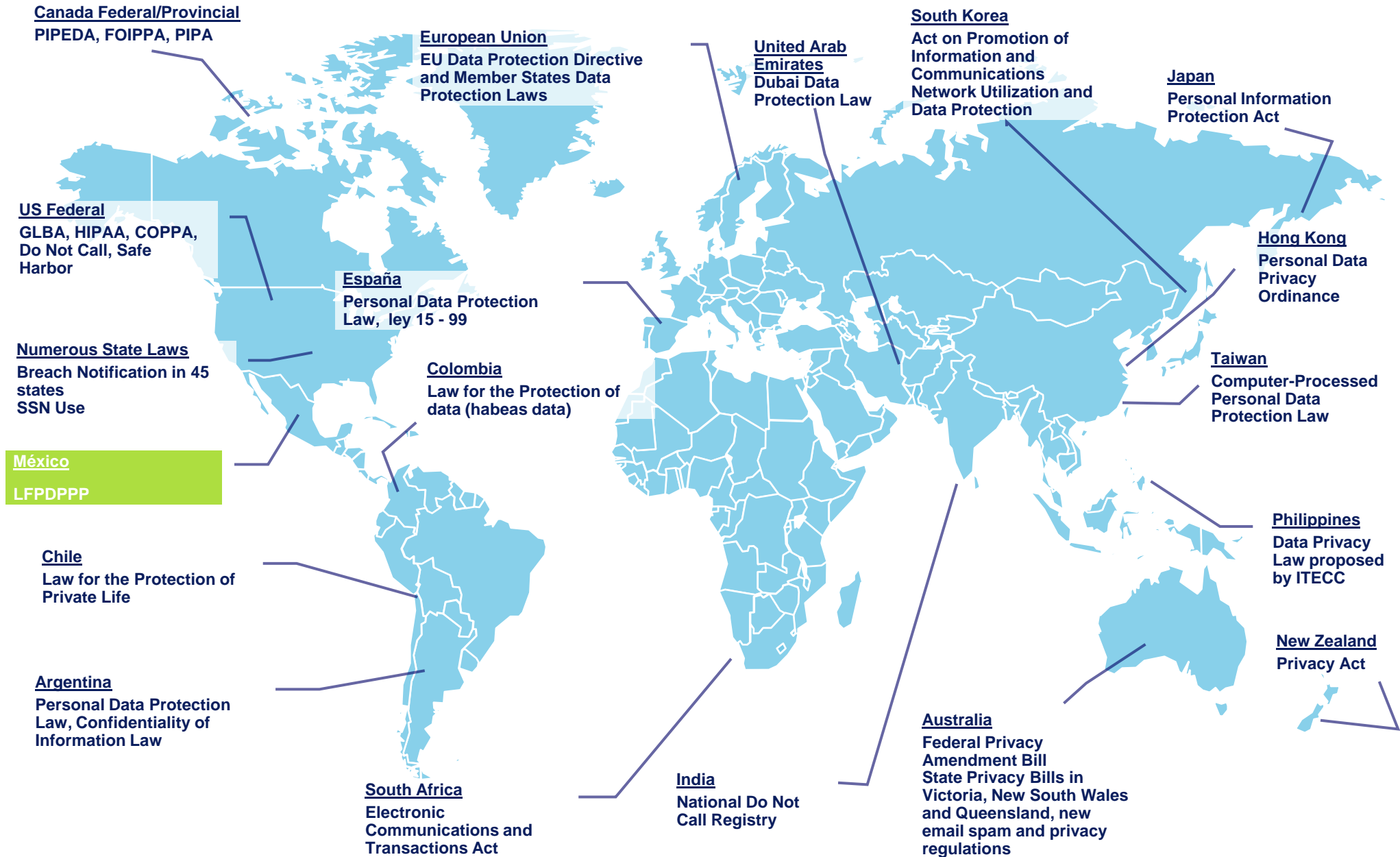
3.- Persona o departamento de datos personales

- Funciones y perfil de la persona de protección de datos
- Perfil de la persona de protección de datos

4.- ¿Por dónde iniciar?

¿Preguntas?

Leyes de Protección de Datos Personales en el Mundo



Introducción

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) emitida el **5 de julio de 2010** conlleva a las empresas a cumplir con nuevos requerimientos. Dichos requerimientos se relacionan con el tratamiento de los datos personales de **clientes, proveedores y empleados** con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

El cumplimiento ante la ley gira alrededor de los mecanismos relacionados con los siguientes temas:

1. Tratamiento de datos personales
2. Protección de datos personales
3. Ejercicio de los derechos ARCO por parte de los titulares.

Introducción (cont.)

Algunos términos importantes:

- **Titular.**- es el dueño de los datos.
- **Responsable.**- encargado de la obtención, tratamiento y cancelación de los datos.
- **Tratamiento.**- La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.
- **Autoridades.**- Instituto Federal de Acceso a la Información y Protección de Datos (IFAI PD) y Secretaría de Economía (SE).
- **Consentimiento.**- Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos (tácito o expreso).
- **Aviso de Privacidad.**- Medio para otorgar el consentimiento que informa al titular sobre el tratamiento de los datos y el ejercicio de los derechos ARCO.
- **Derechos Arco.**- Derechos de los titulares a **A**cceder, **R**ectificar, **C**ancelar u **O**ponerse a la transferencia de sus datos personales.

Dato Personal

Cualquier información concerniente a una persona física identificada o identificable.

Consentimiento será expreso cuando la voluntad se manifieste: verbalmente, escrito, medio electrónico, óptico u otra tecnología. Consentimiento tácito si el Titular no manifiesta oposición.

Dato Personal Sensible

Datos personales que afectan la esfera más íntima de su Titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave. (*Ejemplo: origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.*)

Consentimiento: expreso y por escrito, a través de su firma autógrafa, electrónica o cualquier mecanismo de autenticación.

¿Quién tiene que cumplir con la LFPDPPP?

Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, excepto:

- a. Las sociedades de información crediticia.
- b. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Entre los negocios que pueden ser identificados como sujetos regulados por esta Ley están, desde los grandes bancos, aseguradoras, telefónicas, medios de comunicación, tiendas departamentales y de autoservicio, laboratorios, inmobiliarias y líneas aéreas, hasta escuelas, tintorerías, médicos, dentistas, talleres mecánicos y pizzerías.

Información contenida en el recordatorio publicado por el IFAI PD en el periódico El Norte el 1° de julio, 2011

Principios de Protección de Datos Personales

Licitud

Deben recabarse y tratarse de forma lícita.

Consentimiento

Sujeto al consentimiento del titular.

Información

Debe hacerse del conocimiento del titular.

Calidad

Deben ser pertinentes, correctos y actualizados.

Finalidad

Limitarse al cumplimiento de las finalidades previstas en el aviso.

Lealtad

Respetar la expectativa razonable de privacidad.

Proporcionalidad

El que resulte adecuado, necesario y relevante.

Responsabilidad

Tomar las medidas necesarias y suficientes para el respeto por el responsable y terceros con los que guarde relación jurídica.

Nuestra visión general de la LFPDPPP

Responsable

Titulares



Dueños de los Datos Personales

Terceros



Entidades contratadas por el Responsable para el tratamiento de los datos personales (proveedores).

1.- Obtener los Datos

Consentimiento



Aviso de privacidad

Solicitudes ARCO

Mecanismo por medio del cual los Titulares podrán ejercer sus derechos hacia su información.

Procesos



Punto de contacto de los titulares

TI



Responsable de la implementación de las medidas de protección

Depto. Datos Personales



Legal



Punto de contacto con las autoridades y las áreas internas.

3.- Cancelar los Datos



2.- Mantener los Datos

ISO 27001
DRP (BS25999)
COBIT
ISO 20001



Procesos de requeridos para el Tratamiento de los datos personales:

- Concientización en Seguridad.
- Admón. Seguridad Física
- Admón. de Vulnerabilidades
- Admón. de Riesgos
- Admón. de Incidentes
- Admón. de Control de Acceso
- Admón. de Disponibilidad
- Políticas y Estructuras

Estándares Internacionales de Protección de Datos



Todos los procesos del Responsable alineados a estándares Internacionales de Protección de Datos

Sponsor/Dirección General



Apoyo y definición de directrices requeridas

LFPDPPP

Consta de 69 artículos, distribuidos en XI capítulos



Autoridades



ifai

SECRETARÍA DE ECONOMÍA SE

Responsables de promover el ejercicio de la Ley. Vigilar su cumplimiento.

Principios de Privacidad Generalmente Aceptados

Los Principios de Privacidad Generalmente Aceptados (GAPP por sus siglas inglés) desarrollados por el AICPA y el CICA, proveen una guía para definir buenas prácticas de privacidad y seguridad. Los diez principios de privacidad son los siguientes:

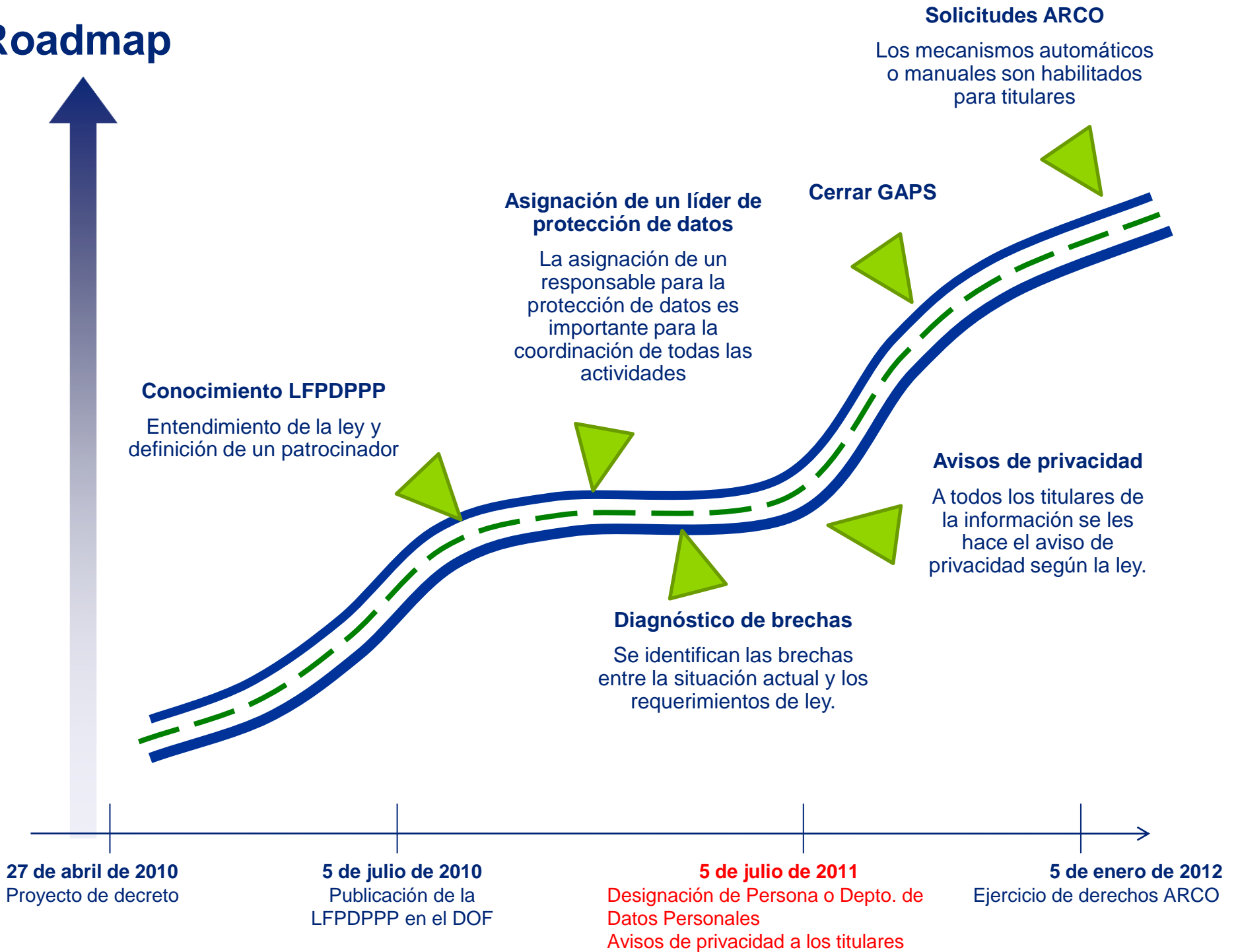
1. Administración
2. Aviso de privacidad
3. Consentimiento
4. Obtención
5. Uso, retención y cancelación
6. Acceso
7. Traspaso a terceros
8. Seguridad y privacidad
9. Calidad
10. Monitoreo

Beneficios de buenos controles de privacidad

Un buen gobierno involucra la identificación de riesgos significativos para la organización (mal uso, filtración o pérdida de datos personales) y el aseguramiento de que se cuenta con los controles apropiados para mitigar estos riesgos. Los beneficios de buenos controles incluyen lo siguiente:

- Protección de la imagen pública y de la marca
- Protección de datos valiosos de clientes, empleados y proveedores
- Logro de ventaja competitiva en el mercado
- Cumplimiento con leyes y regulaciones de privacidad
- Mejora en la credibilidad y promoción de confianza

Roadmap



Aviso de Privacidad

Medio para otorgar el consentimiento que informa al titular sobre el tratamiento de los datos y el ejercicio de los derechos ARCO. Deberá contener, al menos, la siguiente información (art. 16):

1. La **identidad** y **domicilio** del responsable que los recaba;
2. Las **finalidades** del tratamiento de datos;
3. Las **opciones y medios** que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
4. Los **medios** para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
5. En su caso, las **transferencias** de datos que se efectúen, y
6. El **procedimiento y medio** por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.
7. En el caso de datos personales **sensibles**, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

El Aviso de Privacidad también deberá precisar la **persona o departamento** encargado de atender las solicitudes para acceder, rectificar, cancelar u oponerse al uso de datos personales (derechos ARCO).

Modalidades de aviso de privacidad

La Ley permite al responsable simplificar el contenido del aviso de privacidad para fines prácticos, por tanto, se cuenta con dos modalidades de aviso de privacidad previstas en Ley.

Modalidad de aviso	En qué casos se utiliza	Cuándo se debe dar a conocer	Elementos mínimos que debe contener
Completo	Datos recabados de manera personal del titular	Al momento en que se recaban los datos personales, junto al formato de recopilación de los datos	Incluye todos los elementos propios del aviso de privacidad
Simplificado	Datos obtenidos directamente del titular por cualquier medio electrónico, óptico o sonoro	De manera inmediata cuando el titular ingrese al sistema o aplicación mediante el cual se recabarán sus datos	Información sobre identidad y domicilio del responsable, las finalidades del tratamiento y mecanismos para conocer el aviso completo.

* No aplica cuando el tratamiento sea con fines históricos, estadísticos o científicos.

Medidas compensatorias

Las medidas compensatorias son una forma alterna de dar a conocer a los titulares de los datos personales, de manera masiva, la existencia y características del tratamiento de sus datos.



¿QUÉ MEDIDA UTILIZAR?

Elementos a considerar

- El número de titulares
- La antigüedad de los datos
- Su capacidad económica
- Su ámbito territorial o sectorial de operación
- El tipo de medida compensatoria que pretende utilizar.

Medidas recomendadas

- Diario de circulación nacional
- Diario local o revista especializada
- Página de Internet del responsable
- Carteles
- Cápsulas informativas en radio
- Otros medios de comunicación masiva

*El responsable deberá contar con previa autorización del Instituto.

Persona o departamento de datos personales

El **artículo 30** de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, establece la obligación de los responsables del tratamiento de datos personales, de **designar** a una persona o departamento de datos personales.

El nivel de adopción de las recomendaciones que se presentan, podrá variar de organización en organización dependiendo de su tamaño, capacidad y necesidades.



Persona o departamento de datos personales (cont.)

¿Persona o departamento?

La primer decisión para la designación de la función de protección de datos personales, será elegir si estará a cargo de una persona o un departamento. Para ello, se recomienda considerar lo siguiente:

Evaluar:

- Tipo y cantidad de datos personales que trata,
- Naturaleza e intensidad del tratamiento,
- Número potencial de solicitudes de titulares de datos personales que podrá recibir

Decidir a quién se designará:

- El propio responsable, cuando se trate de una persona física
- Una persona designada por el responsable, que puede ser parte de la estructura o negocio del responsable, o bien un encargado
- Un departamento de la organización



Funciones de la persona de protección de datos

Funciones de la persona o departamento

- Dar trámite a las solicitudes de los titulares de datos personales para el ejercicio de los derechos a los que refiere la Ley.
- Fomentar la protección de datos personales al interior de la organización del responsable.

Sugerencias de funciones para asegurar el cumplimiento

- Establecer y administrar **procedimientos** para la recepción, tramitación, seguimiento y atención oportuna de las solicitudes para el ejercicio de los derechos **ARCO**.
- Monitorear los avances o cambios **legislativos** en materia de privacidad y protección de datos personales.
- Diseñar y ejecutar una **política y/o prácticas** de protección de datos personales, alinearla a los procesos internos de la organización, difundir y comunicarla, así como desarrollar un mecanismo para evaluar su eficacia y eficiencia
- Identificar e implementar **mejores prácticas** relacionadas con la protección de datos personales
- Ser el **representante** de la organización en materia de protección de datos personales ante otros actores.

Perfil de la persona de protección de datos

Perfil de la persona de protección de datos

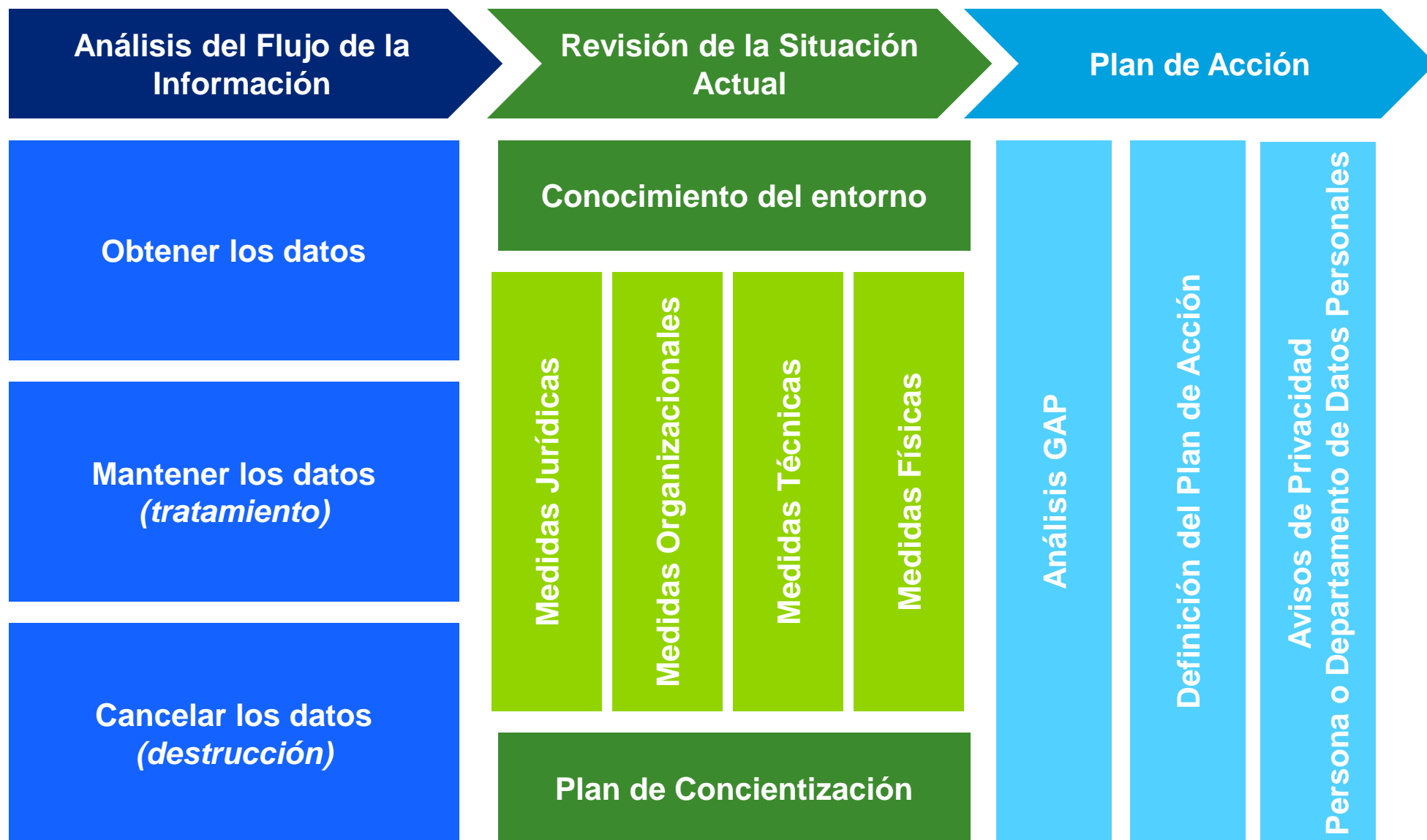
- Experiencia en materia de protección de datos personales
- Jerarquía o posición indicada dentro de la organización
- Recursos suficientes (materiales, técnicos y humanos) para el ejercicio de sus funciones y acciones
- Contar con conocimiento en la materia
- Visión y liderazgo
- Habilidades de organización y comunicación

Nombres sugeridos

- Oficial de Protección de Datos Personales
- Departamento de Protección Datos Personales
- Persona Designada para la Protección de Datos Personales

¿Por dónde iniciar?

Primeros pasos



¿Preguntas?

Contactos

- **Eduardo Cocina Hernández, CISA, CGEIT**
Socio
Tel. (52) 5080-6936
ecocina@deloittemx.com
- **Alberto Durán Jacinto, CISA, CISM**
Director
Tel. (81) 8133-7329
aduran@deloittemx.com
- **José González Saravia, CPA**
Socio
Tel. (52) 5080-6722
jgonzalezsaravia@deloittemx.com
- **Mayra Rivera Marchesini, CISA, CGEIT**
Gerente
Tel. (81) 8133-7505
mrivera@deloittemx.com
- **Salomón Rico Baños, CISA, CISM, CGEIT**
Socio
Tel. (81) 8133-7351
srico@deloittemx.com
- **Miguel Ishii**
Jones Day
Tel. (52) 3000-4000
Mishii@jonesday.com

Deloitte.