

## Cumplimiento con la LFPDPPP Technology Risk Services



Enero 26, 2012

Mayra Rivera Marchesini, CISA, CGEIT, CRISC

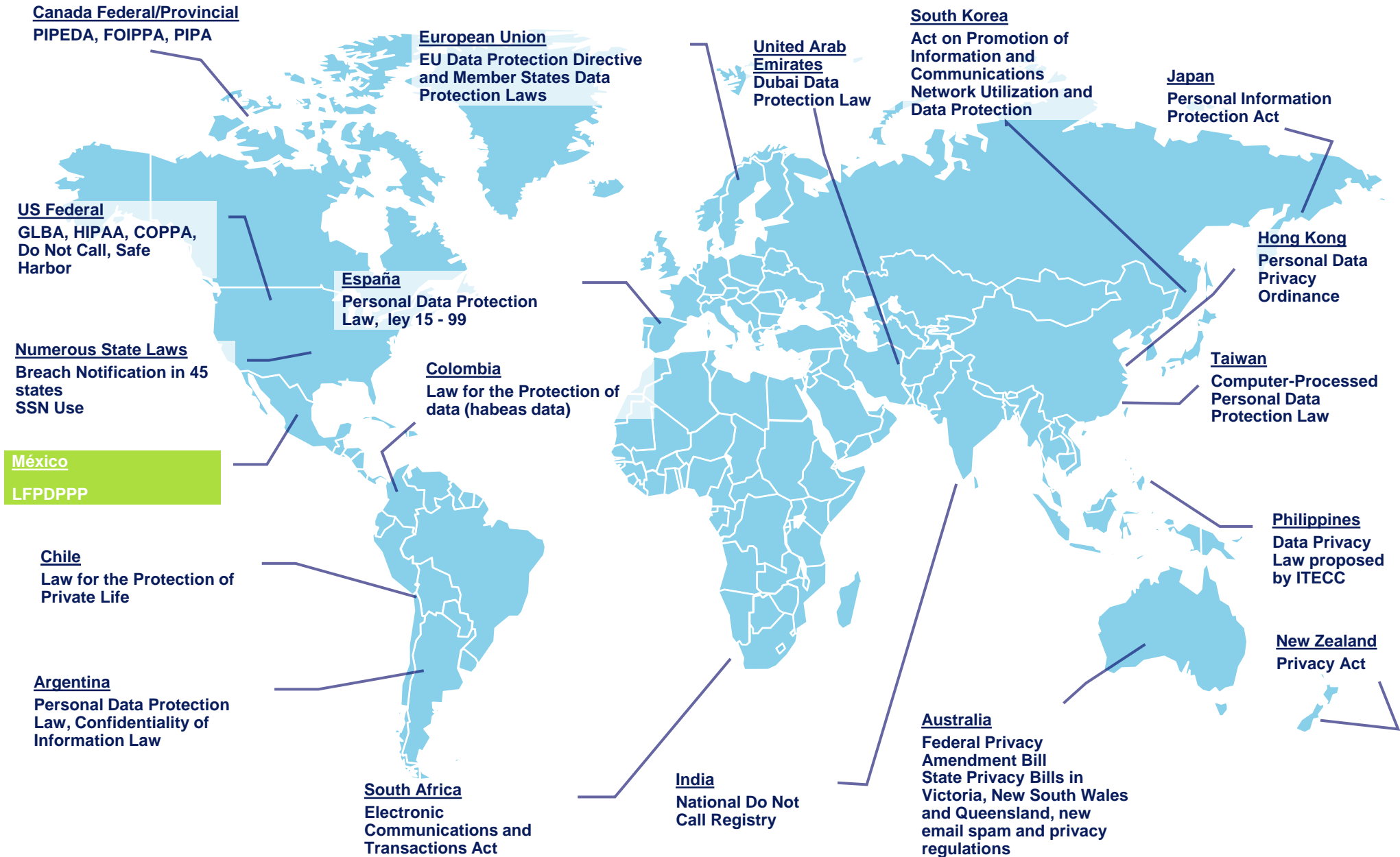
Gerente ERS

# Contenido

- Leyes de Protección de Datos Personales en el Mundo
- ¿Qué es la LFPDPPP?
- Roadmap
- Ley y reglamento
- Requisitos para el cumplimiento con la LFPDPPP
- Acciones para la seguridad de los datos personales
- Remisiones vs. Transferencias
- Modelo de implementación
- Modelo de madurez de privacidad
- Infracciones
- ¿Preguntas?

# Introducción

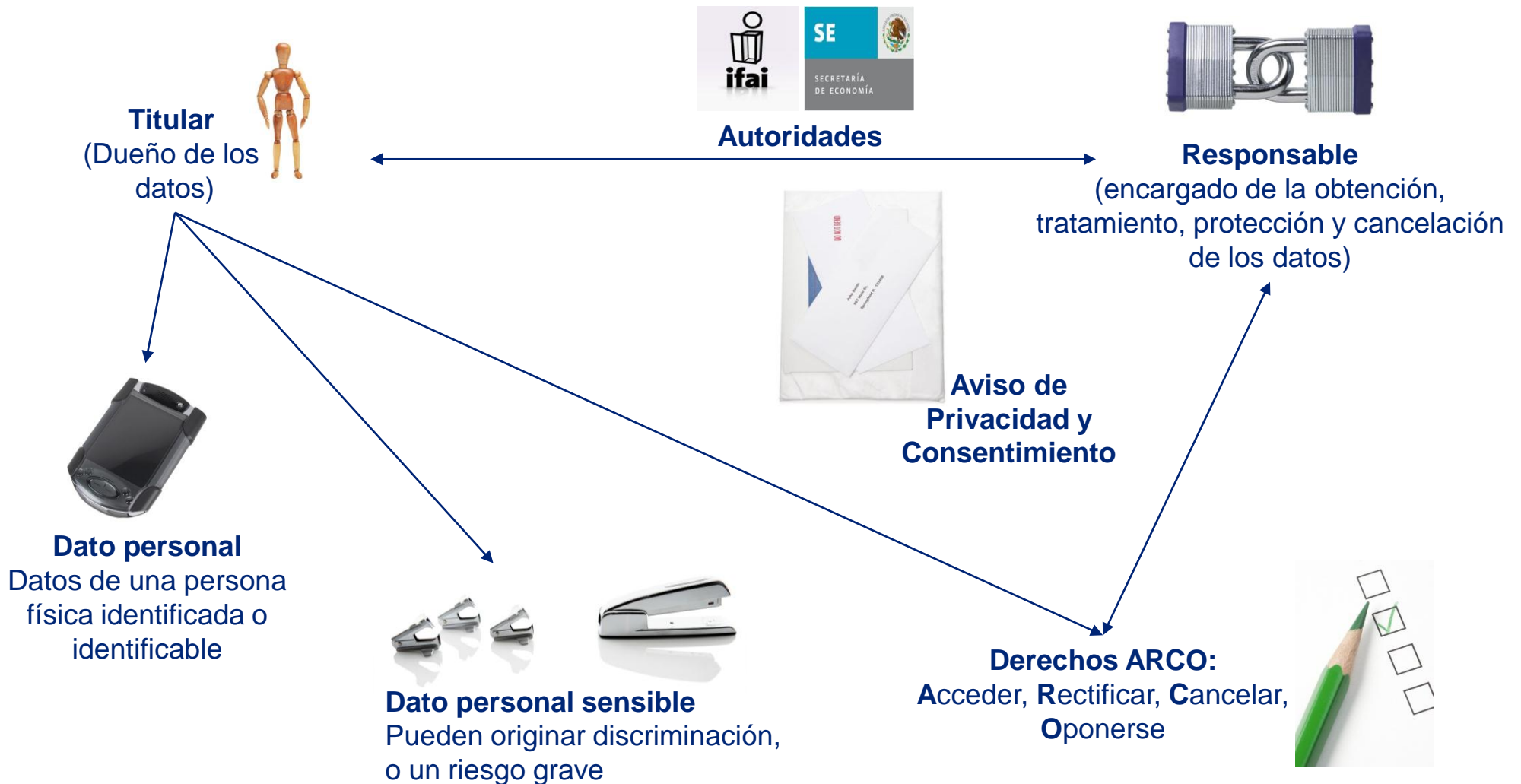
# Leyes de Protección de Datos Personales en el Mundo



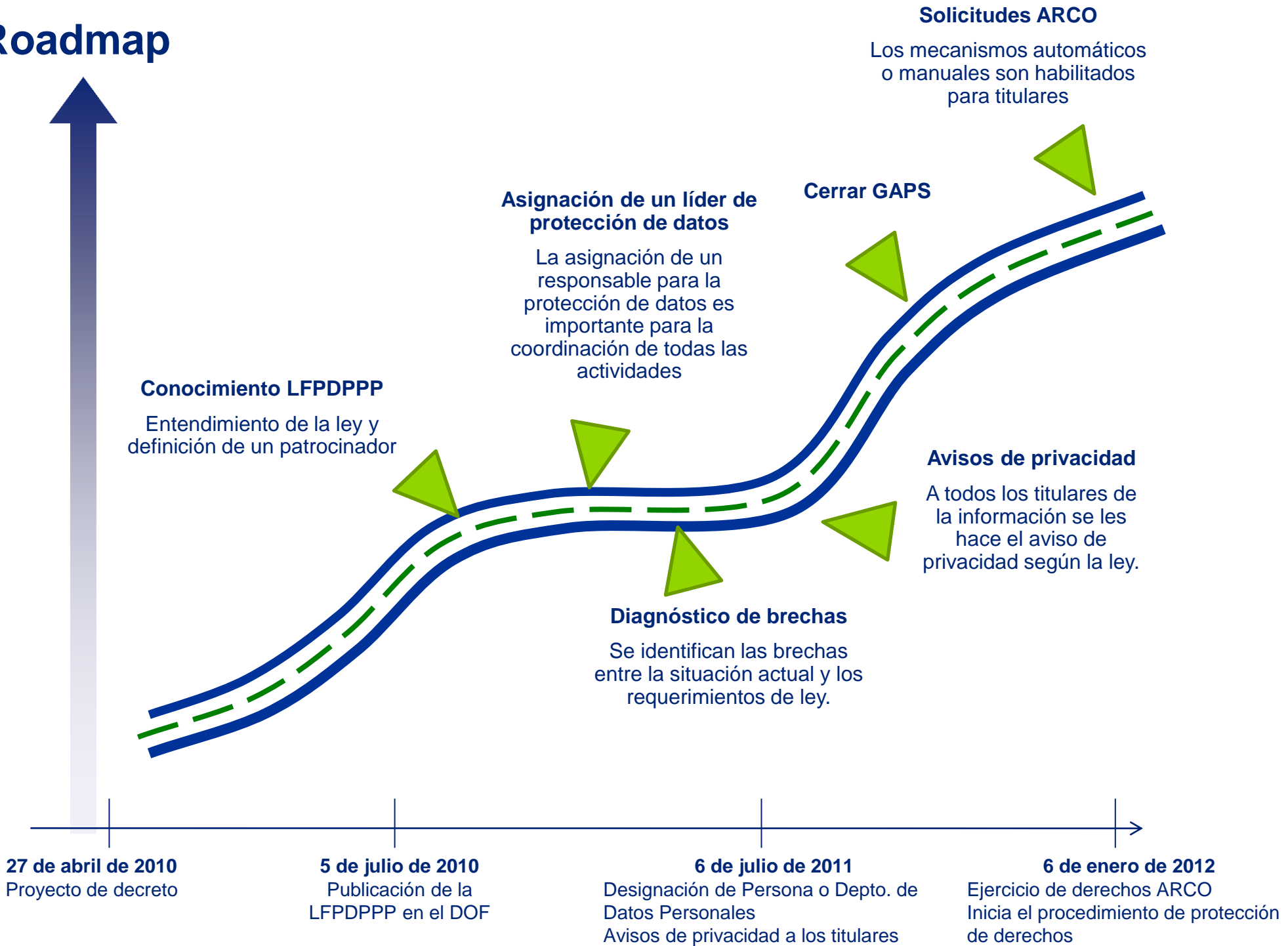
# ¿Qué es la LFPDPPP?

Publicada el pasado 5 de julio de 2010 en el DOF, tiene como objetivo proteger datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de los individuos.

Algunos términos y conceptos importantes:



# Roadmap



# Ley y reglamento

- La **ley** indica lo que se debe hacer
- El **reglamento** dice bajo que reglas se debe hacer lo que indica la ley
- Cada responsable debe establecer el **cómo** cumplir

# Requisitos para el cumplimiento con la LFPDPPP

# Requisitos para el cumplimiento con la LFPDPPP

1. Avisos de Privacidad
2. Persona o departamento responsable de datos personales
3. Derechos ARCO
4. Protección de datos personales
5. Vulneraciones de seguridad
6. Políticas y procedimientos de privacidad
7. Relación entre el responsable y el encargado y/o tercero (cláusulas contractuales)
8. Cláusula de privacidad para los empleados
9. Cláusula a agregar a los contratos de confidencialidad

# Acciones para la seguridad de los datos personales

# ¿Qué acciones tomar para la seguridad de los datos personales?

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

## 1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales

2. Determinar las funciones y obligaciones de las personas que traten datos personales
3. Contar con un análisis de riesgos de datos personales
4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva
5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes
6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes
7. Llevar a cabo revisiones y/o auditorías
8. Capacitar al personal que trate datos personales
9. Realizar un registro de los medios de almacenamiento de los datos personales



# ¿Qué acciones tomar para la seguridad de los datos personales? (2)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales

## 2. Determinar las funciones y obligaciones de las personas que traten datos personales

3. Contar con un análisis de riesgos de datos personales

4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva

5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes

6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes

7. Llevar a cabo revisiones y/o auditorías

8. Capacitar al personal que trate datos personales

9. Realizar un registro de los medios de almacenamiento de los datos personales



# ¿Qué acciones tomar para la seguridad de los datos personales? (3)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales
2. Determinar las funciones y obligaciones de las personas que traten datos personales

## 3. Contar con un análisis de riesgos de datos personales

4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva
5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes
6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes
7. Llevar a cabo revisiones y/o auditorías
8. Capacitar al personal que trate datos personales
9. Realizar un registro de los medios de almacenamiento de los datos personales



# ¿Qué acciones tomar para la seguridad de los datos personales? (4)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales
2. Determinar las funciones y obligaciones de las personas que traten datos personales
3. Contar con un análisis de riesgos de datos personales

## 4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva

5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes
6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes
7. Llevar a cabo revisiones y/o auditorías
8. Capacitar al personal que trate datos personales
9. Realizar un registro de los medios de almacenamiento de los datos personales



# ¿Qué acciones tomar para la seguridad de los datos personales? (5)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales
2. Determinar las funciones y obligaciones de las personas que traten datos personales
3. Contar con un análisis de riesgos de datos personales
4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva
- 5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes**
6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes
7. Llevar a cabo revisiones y/o auditorías
8. Capacitar al personal que trate datos personales
9. Realizar un registro de los medios de almacenamiento de los datos personales



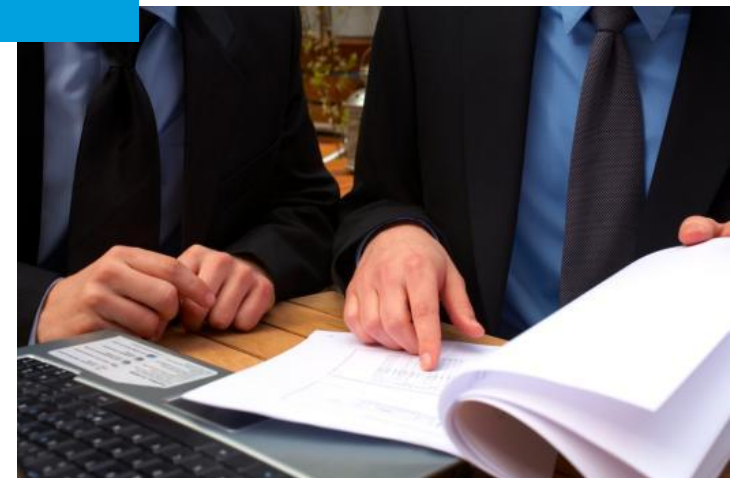
# ¿Qué acciones tomar para la seguridad de los datos personales? (6)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales
2. Determinar las funciones y obligaciones de las personas que traten datos personales
3. Contar con un análisis de riesgos de datos personales
4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva
5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes

## 6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes

7. Llevar a cabo revisiones y/o auditorías
8. Capacitar al personal que trate datos personales
9. Realizar un registro de los medios de almacenamiento de los datos personales



# ¿Qué acciones tomar para la seguridad de los datos personales? (7)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales
2. Determinar las funciones y obligaciones de las personas que traten datos personales
3. Contar con un análisis de riesgos de datos personales
4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva
5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes
6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes

## 7. Llevar a cabo revisiones y/o auditorías

8. Capacitar al personal que trate datos personales
9. Realizar un registro de los medios de almacenamiento de los datos personales



# ¿Qué acciones tomar para la seguridad de los datos personales? (8)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales
2. Determinar las funciones y obligaciones de las personas que traten datos personales
3. Contar con un análisis de riesgos de datos personales
4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva
5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes
6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes
7. Llevar a cabo revisiones y/o auditorías

## 8. Capacitar al personal que trate datos personales

9. Realizar un registro de los medios de almacenamiento de los datos personales



# ¿Qué acciones tomar para la seguridad de los datos personales? (9)

El responsable deberá elaborar una relación de medidas de seguridad tomando en cuenta las siguientes acciones, así como a las personas que realizarán cada función de seguridad:

1. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales
2. Determinar las funciones y obligaciones de las personas que traten datos personales
3. Contar con un análisis de riesgos de datos personales
4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva
5. Realizar un análisis de brechas entre las medidas de seguridad existentes y las faltantes
6. Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes
7. Llevar a cabo revisiones y/o auditorías
8. Capacitar al personal que trate datos personales

**9. Realizar un registro de los medios de almacenamiento de los datos personales**



# Remisiones vs. Transferencias

# Remisiones vs. Transferencias

| Encargado  | Tercero   |
|--|---|
| La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.         | La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.  |
| Remisión: La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano; | Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.   |
| Las remisiones no requerirán ser informadas al titular ni contar con su consentimiento. (Artículo 53 - Reglamento)         | Toda transferencia de datos personales se encuentra sujeta al consentimiento de su titular. Deberá ser informada a este último mediante el aviso de privacidad y limitarse a la finalidad que la justifique. (Artículo 68 - Reglamento) |

# Modelo de implementación

# Modelo de implementación del Programa de Privacidad de Datos

Nuestro modelo se basa en Principios Internacionales de Privacidad Generalmente Aceptados, e integra los conceptos clave de la LFPDPPP para crear un Programa de Privacidad efectivo que cubra las obligaciones de la Ley desde la perspectiva de tecnología, procesos, gente y legal, a través de las siguientes fases:



Principios de Privacidad Generalmente Aceptados / Requerimientos LFPDPPP / BS 10012 / ISO 27000

# Modelo de Madurez de Privacidad

# Modelo de Madurez de Privacidad

El **modelo de madurez** es un recurso que permitirá, evaluar y medir el progreso, en aspectos de cumplimiento, contra los requerimientos establecidos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (traducidos en principios y criterios de privacidad).

Las ventajas de un modelo de madurez, incluyen:

- Fortalecer a la organización durante las etapas relacionadas con el “logro del cumplimiento”.
- Permitir que la organización identifique el nivel aceptable para cumplir con los requerimientos con base en sus recursos.
- Obtener diversos valores y beneficios, conforme la organización consigue un mayor nivel de madurez.

El modelo de madurez de privacidad (PMM por sus siglas en inglés) de AICPA/CICA se basa en los GAPP (General Accepted Privacy Principles) y en el CMM (Capability Maturity Model).

## Modelo de Madurez de Privacidad (cont.)

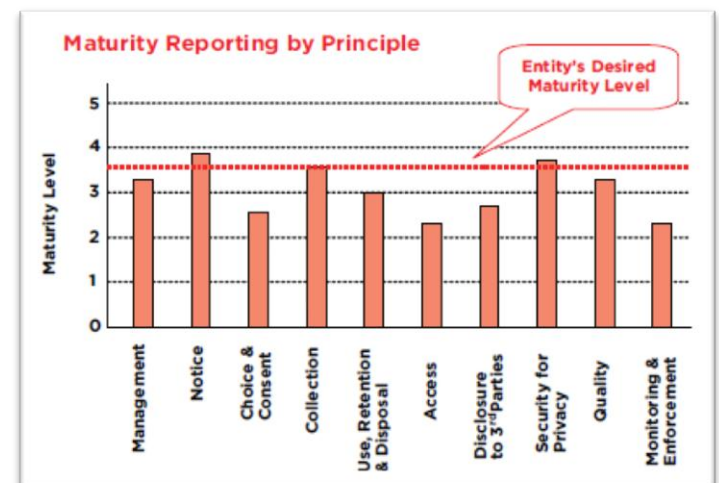
Los Principios de Privacidad Generalmente Aceptados (GAPP por sus siglas inglés) desarrollados por el AICPA y el CICA, proveen una guía para definir buenas prácticas de privacidad y seguridad. Los diez principios de privacidad son los siguientes:

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

# Modelo de Madurez de Privacidad (cont.)

El PMM utiliza cinco niveles de madurez:

- 1. Ad hoc** – Los procedimientos o procesos generalmente son **informales**, **incompletos** y aplicados de **inconsistente**.
- 2. Repetible** – Existen procesos y procedimientos, sin embargo, no están **completamente** documentados y no consideran **todos** los aspectos relevantes.
- 3. Definido** – Los procesos y procedimientos están completamente documentados e implementados, y cubren todos los aspectos relevantes.
- 4. Administrado** – Se llevan a cabo **revisiones** para evaluar la **eficacia** de los controles implementados.
- 5. Optimizado** – Se llevan a cabo revisiones regulares y procedimientos de retroalimentación para asegurar la **mejora continua** de los procesos involucrados.



# Infracciones

# Infracciones

## Apercibimiento (aviso)

1. No cumplir con la **solicitud ARCO** del titular, sin razón fundada, en los términos previstos en la Ley

## Multa de 100 a 160,000 salarios mínimos

1. Actuar con negligencia o dolo en la **tramitación y respuesta** de solicitudes ARCO
2. Declarar dolosamente la **inexistencia** de datos personales
3. Dar tratamiento a los datos personales en **contravención a los principios** de la Ley
4. Omitir en el **aviso de privacidad**, alguno o todos los elementos
5. Mantener datos personales **inexactos**
6. No cumplir con el **apercibimiento** (para que el responsable lleve a cabo los actos solicitados por el titular)

# Infracciones (cont.)

## Multa de 200 a 320,000 salarios mínimos

1. Incumplir el deber de **confidencialidad**
2. Cambiar sustancialmente la **finalidad** original sin cumplir con el art. 12 (tratamiento limitado a la(s) finalidad(es) descritas en el aviso de privacidad)
3. Transferir datos a **terceros** sin comunicar a éstos el aviso de privacidad
4. Vulnerar la **seguridad** de bases de datos
5. Llevar a cabo la **transferencia o cesión** de los datos personales, fuera de los casos en que esté permitida por la Ley
6. Recabar o transferir datos personales sin el **consentimiento** expreso del titular, en los casos en que éste sea exigible
7. Obstruir los actos de **verificación** de la autoridad
8. Recabar datos en forma **engañosa y fraudulenta**
9. Continuar con el **uso ilegítimo** de los datos personales cuando se ha solicitado el cese
10. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos **ARCO**
11. Crear **bases de datos** en contravención al consentimiento de los datos sensibles
12. Cualquier **incumplimiento** del responsable a las obligaciones establecidas a su cargo

## Infracciones (cont.)

### 3 meses a 3 años de prisión

- Al que estando autorizado para tratar datos personales, con **ánimo de lucro**, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

### 6 meses a 5 años de prisión

- Se sancionará al que, con el fin de alcanzar un **lucro indebido**, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

¿Preguntas?

# Contactos

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

---

**Deloitte.**