Deloitte.

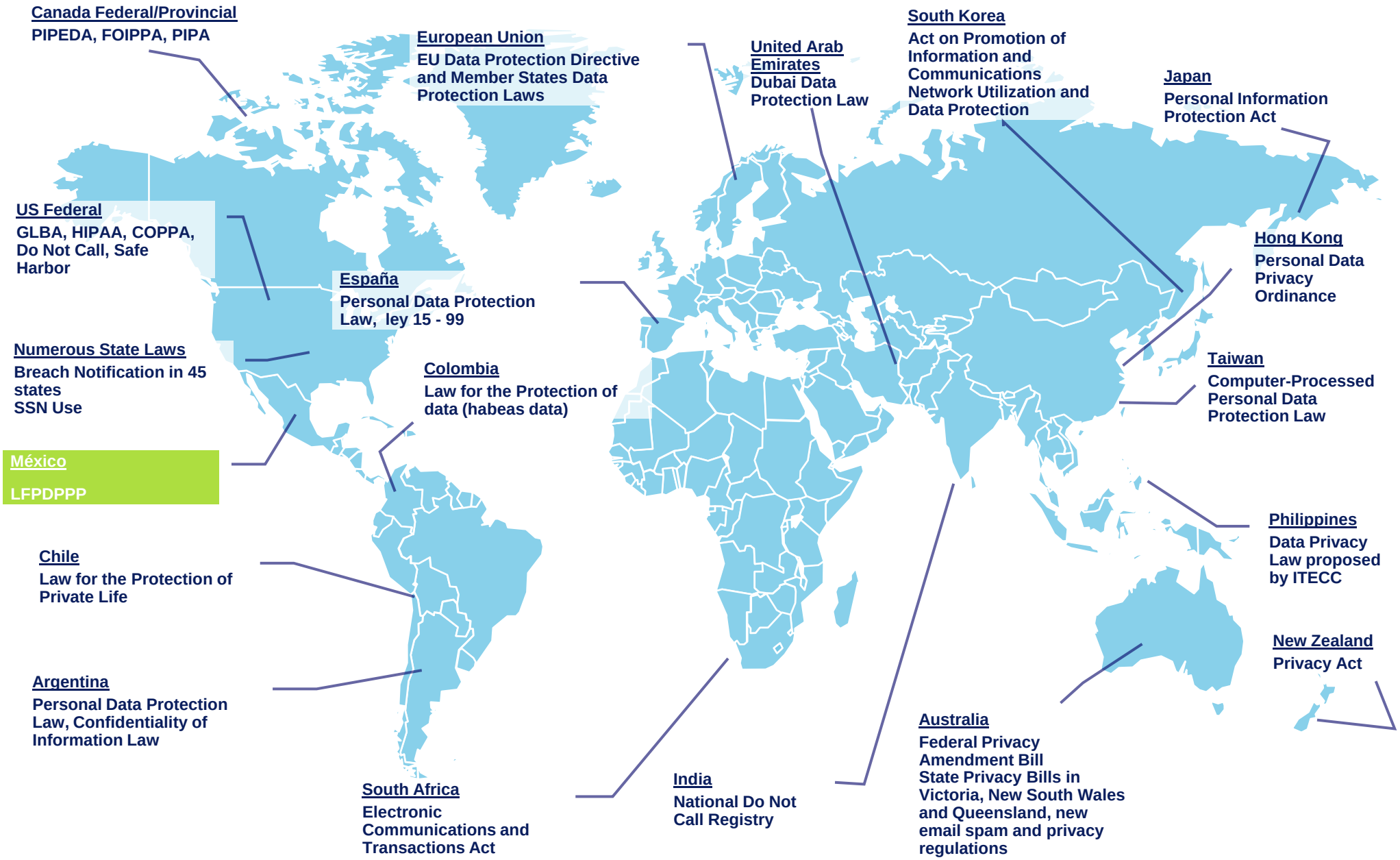
Alineación a la LFPDPPP
Information & Technology Risk Services

Noviembre, 2010

Consultoría México /
Technology and Information Risk Services

Contenido

Leyes de Protección de Datos Personales en el Mundo



Introducción

Como es de su conocimiento, el pasado **5 de julio de 2010 se publicó** en el Diario Oficial de la Federación (DOF) la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual tiene como objetivo proteger los 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 importantes:
  - Titular.- es el dueño de los datos
  - Responsable.- encargado de la obtención, tratamiento y cancelación de los datos
  - Autoridades.- IFAI PDP y Secretaría de Economía
  - Datos personales y sensibles

Dato Personal	Dato Personal Sensible
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.	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.

Consentimiento

Formas

- Tácito: Cuando no manifiesta oposición
- Expreso: Cuando se manifiesta por signos inequívocos
- Por escrito: Mediante firma

Excepciones

- Previsto en una ley
- Figuren en fuentes de acceso público
- Se sometan a un procedimiento de disociación
- Para cumplir obligaciones derivadas de una relación jurídica
- Situación de emergencia
- Indispensables para la atención médica.
- Mediante resolución de autoridad.

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).

Introducción

Estructura de la LFPDPPP

I. Disposiciones Generales	II. Los Principios de Protección de Datos Personales
III. Los Derechos de los Titulares de Datos Personales	IV. Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición - ARCO
V. De la Transferencia de Datos	VI. Las Autoridades Sección I. Del Instituto Sección II. De las Autoridades Reguladoras
VII. Del Procedimiento de Protección de Derechos	VIII. Del Procedimiento de Verificación
IX. Del Procedimiento de Imposición de Sanciones	X. De las Infracciones y Sanciones → Conductas de los Responsables que constituyen infracciones de la Ley.
XI. De los Delitos en Materia del Tratamiento Indebido de Datos Personales → Art. 67, Art. 68, Art. 69	
Transitorios	

Derechos ARCO

Los titulares tienen derecho a:

- **Acceder** a sus datos personales.
- **Rectificar** inexactitudes en sus datos personales.
- **Cancelar** sus datos personales.
- **Oponerse** a la transferencia de sus datos personales.

Los titulares podrán reclamar la protección de los derechos ARCO mediante procedimientos ante el IFAI PDP.

¿Quién tiene que cumplir con la LFPDPPP?

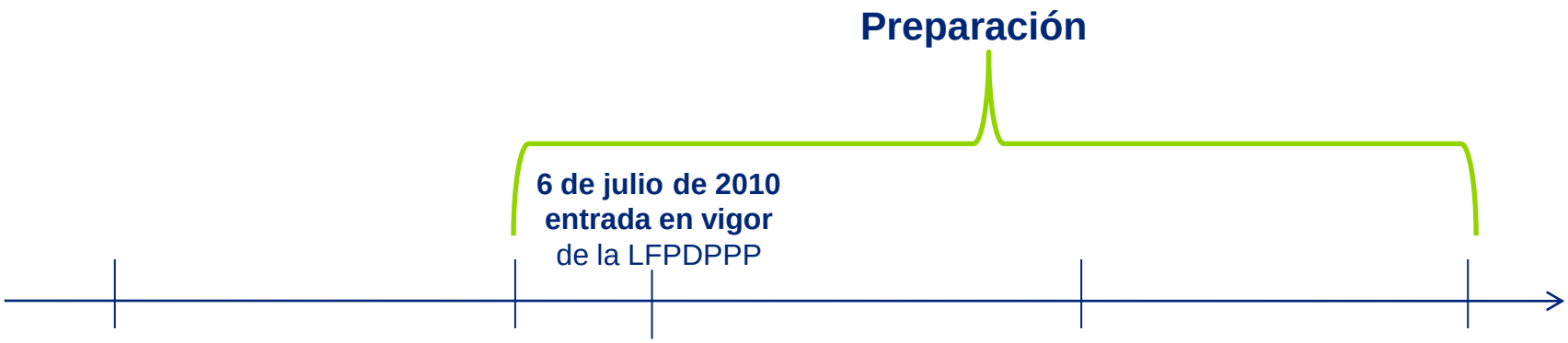
Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, excepto:

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.

Línea de tiempo

Algunas de las fechas claves de la LFPDPPP



27 de abril de 2010
Proyecto de decreto

5 de julio de 2010
Publicación de la LFPDPPP en el DOF

5 de julio de 2011
Designación de Persona o Depto. de Datos Personales

Avisos de privacidad a los titulares

5 de enero de 2012
Ejercicio de derechos ARCO

Inicia el procedimiento de protección de derechos

Nuestra visión general de la LFPDPPP

Punto de vista

Macroprocesos

Actores

Principios

Licitud
Consentimiento
Información
Calidad
Finalidad
Lealtad
Proporcionalidad
Responsabilidad

Obtener los datos

Mantener los datos

Cancelar los datos

Tecnología

Procesos

Legal

Gobierno, riesgos, cumplimiento

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 LFPDP

Principales actores

Es necesaria para la implementación **de medidas administrativas, técnicas y físicas para proteger la seguridad de los datos**, basadas en un análisis de riesgos. Su participación es importante para la administración de disponibilidad, vulnerabilidades e incidentes.

Área de TI

IFAI PDP SE

Área legal

Es el punto de contacto con las autoridades y las áreas internas.

Participación en el diseño, implementación y gestión de las actividades para el cumplimiento de los requerimientos.

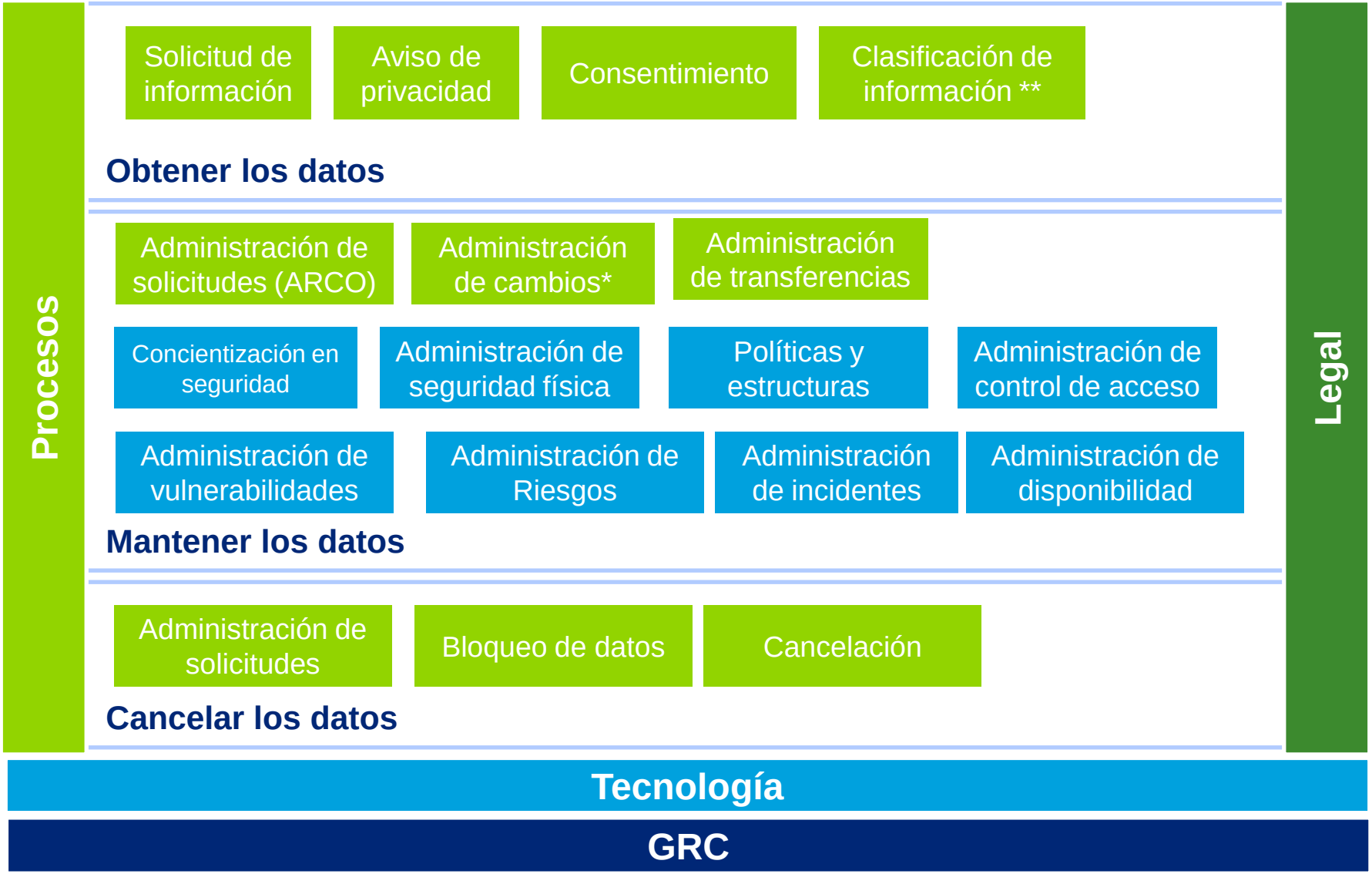
Áreas de GRC

Punto de contacto de los titulares para dar respuesta entre otras a las solicitudes ARCO (Acceso, rectificación, cancelación y oposición). Además de su participación en la obtención de la información (Aviso de privacidad, Consentimiento)

Procesos de negocio

Titulares

Nuestra visión general de la LFPDPPP



** La clasificación de la información se refiere a identificar datos sensibles según la Ley.

* Administración de cambios se refiere a cambios en finalidad.

Procesos que se podrían basar en estándares int. como ISO27001, DRP (BS25999), COBIT, ITIL, SOX, ISO2000, estándares de la APEC.

De la Transferencia de Datos

- Debe comunicarse el aviso de privacidad
- Conforme a la opción del titular en el aviso de privacidad
- No se requiere consentimiento si la transferencia:
  - Está prevista en una ley o tratado.
  - Sea necesaria para la prevención, diagnóstico o servicios médicos o sanitarios.
  - Se hace a afiliadas que operen bajo los mismos procesos y políticas internas.
  - Se haga por virtud de un contrato en interés del titular.
  - Sea necesaria para la salvaguardia de un interés público.
  - Sea necesaria para el reconocimiento o ejercicio de un derecho procesal.
  - Sea precisa para el mantenimiento o cumplimiento de una relación jurídica con el titular.

Roadmap

La realidad de la Protección de datos en México

La realidad de la protección de datos en México

En la actualidad empresas de todos los tipos, sectores, y tamaños trabajan con una materia prima en común:

Datos Personales (empleados, clientes)
Datos Comerciales (precios, acuerdos, descuentos)
Datos de terceros (información de competencia, proveedores, clientes)
Datos de negocio (metodologías, propiedad intelectual, resultados, estrategias)

A pesar de que la mayoría de las empresas consideran que sus datos o información representan un activo crítico para el cumplimiento de sus objetivos, son pocos los casos en la que éstos han sido identificados, evaluados, y protegidos correctamente. Lo anterior principalmente por la falta de información relativa a las amenazas, y el falso sentido de "protección" derivado de la falla en la identificación de vulnerabilidades.

La falta y/o laxitud de leyes, y normatividad en general, que regulen los procesos de adquisición, procesamiento, almacenamiento y destrucción de datos, también ha provocado que los datos sensibles no sean correctamente protegidos.

La realidad de la protección de datos en México

México: Venta de bases de datos oficiales del Gobierno, información de millones de mexicanos; IFE, Casetas Telmex, Registro de vehículos: Tepito

La mensajería instantánea acelera el peligro del robo de datos

Expide Segob Ley Federal de Protección de Datos Personales

Nacional - Lunes 5 de julio (10:06 hrs.)

CRONICA DE UN ROBO DE DATOS ANUNCIADO; CONTADORES TAMBIEN VENDEN SUS BASES

Por Agencias, 23/04/2010 07:22

Se hace llamar "Licenciado Félix Ortega", y encontrarlo no es nada difícil. Con sólo un clic aparecen los anuncios que puso en internet: "Vendo bases de datos de contadores públicos, garantizo información actualizada al 2010. Datos reales, varios estados y área metropolitana".

2 Jul 2010 - Aumenta el interés de Pymes por soluciones de seguridad - El ...
... por seguir protegiendo sus operaciones obedece a que el 42 por ciento de ellas fue en algún momento objeto del **robo** de su **información** privilegiada. ...
www.elfinanciero.com.mx/elfinanciero/portal/.../contentmgr.cfm?...

Exigen investigar robo de datos que vende Tepito

IFAI urge a indagar en dependencias red de funcionarios que trafica con datos oficiales; IFE detalla que se trata de un delito que debe perseguir la PGR

Empresas pierden 8 mdd por robo de datos

Consideran que resulta imprescindible y benéfica la aprobación de la Ley Federal de Datos Personales en Posesión de Particulares

Profeco multa a Gayosso por $3 millones

Fecha: 2010-05-13

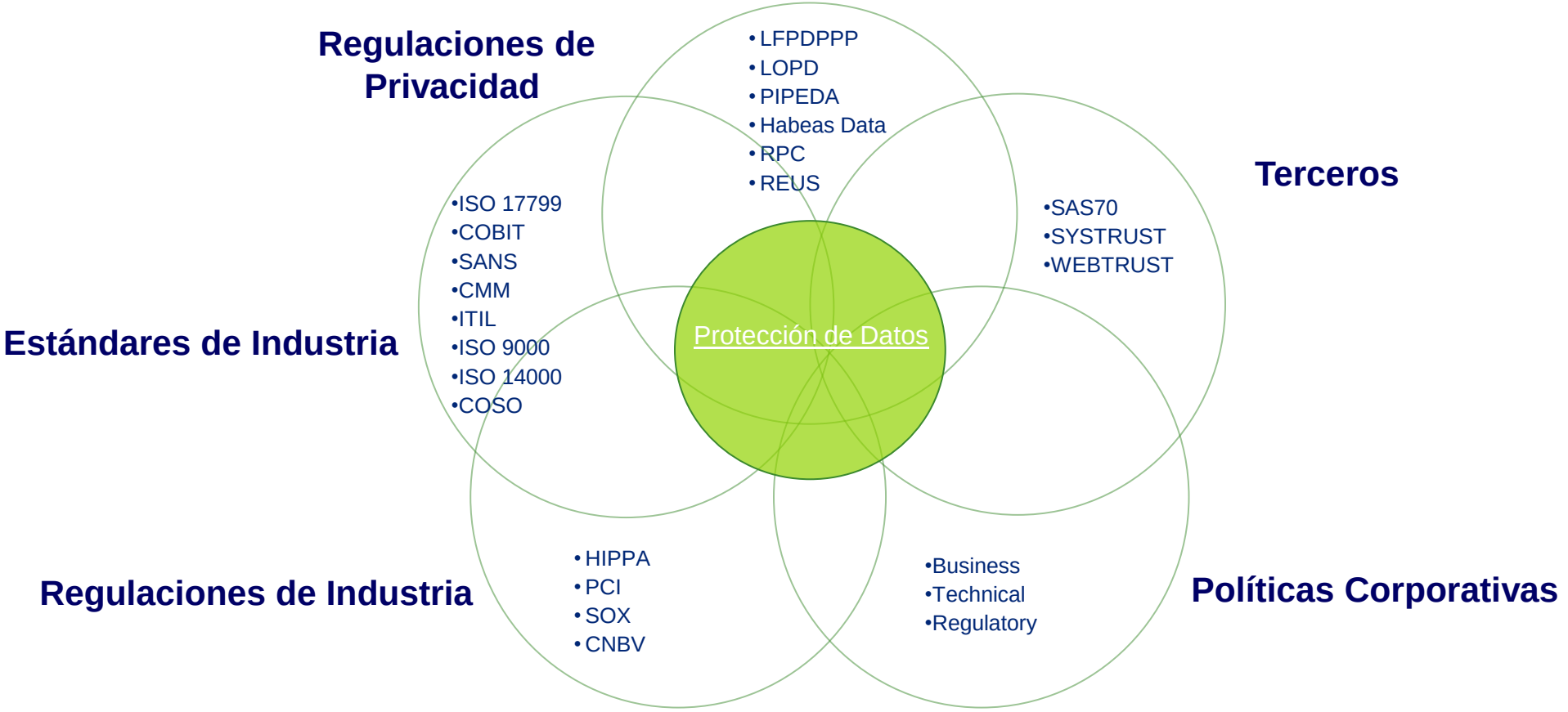
Fuga de datos, *coco* de Pymes

El 75% de la pérdida de información es por robo o extravío de *laptops*, *USB* o errores al enviar correos

Pregunta del día:

Cumplimiento

Las regulaciones globales y locales están creciendo en volumen y en complejidad. Como resultado, la demanda de responsabilidad legal a los Consejos de Accionistas así como a otros órganos de gobierno y, directamente a los ejecutivos se ha intensificado, a la vez que la administración de los costos asociados a la gestión de riesgo y cumplimiento continúa siendo un reto.



Con un enfoque de probar una sola vez en vez de varias veces reduce riesgos y costos

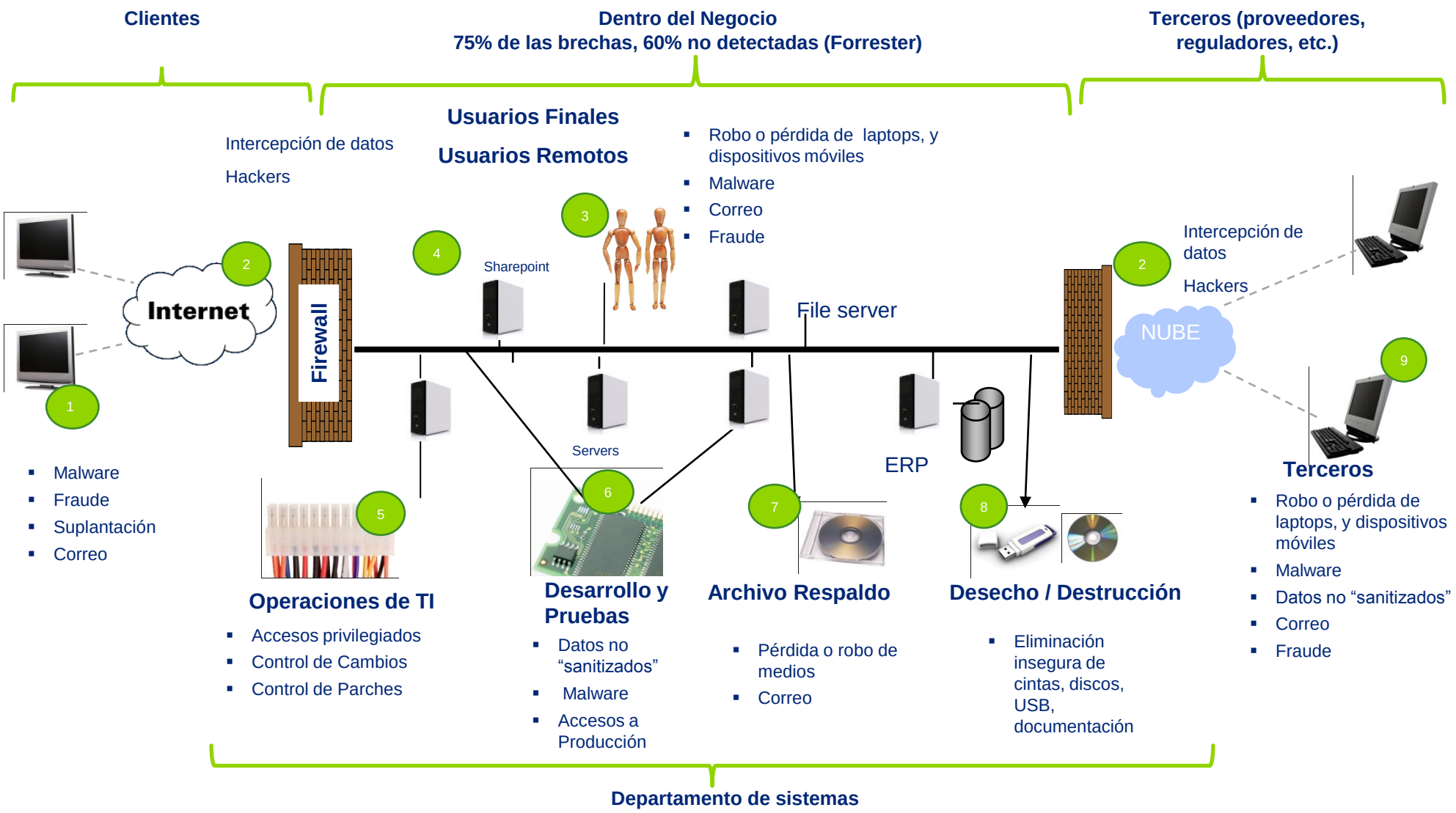
¿Y la realidad de la protección de datos en su Organización?

La realidad en su Organización en 10 simples preguntas…

- ¿Tienen identificados los activos de información críticos para el negocio?
- ¿Hay información en su negocio que pueda ser de interés para terceros?
- ¿Saben cuánto podría costar una fuga de información?
- ¿Tienen identificados los flujos internos y externos por donde se mueve y almacena su información?
- ¿Los empleados conocen sus responsabilidades sobre la protección de información?
- ¿Tienen forma de controlar la reproducción, física o electrónica, de información importante para el negocio?
- ¿Puede identificar qué tipo de información se envía a través del correo electrónico?
- ¿Tienen implementados controles sobre dispositivos móviles (laptops, smartphones, discos duros, memorias USB)?
- ¿Están o estarán sujetos a alguna normatividad o ley que regule la protección de datos?
- ¿Tienen certeza de que no se han presentado fugas de información en su organización?

Puntos de Riesgo

En una organización cualquiera, las amenazas y vulnerabilidades son muy variables, sin embargo, es posible categorizarlas en 9 áreas comunes de riesgo:



Consecuencias de una fuga o pérdida de información

Intangibles

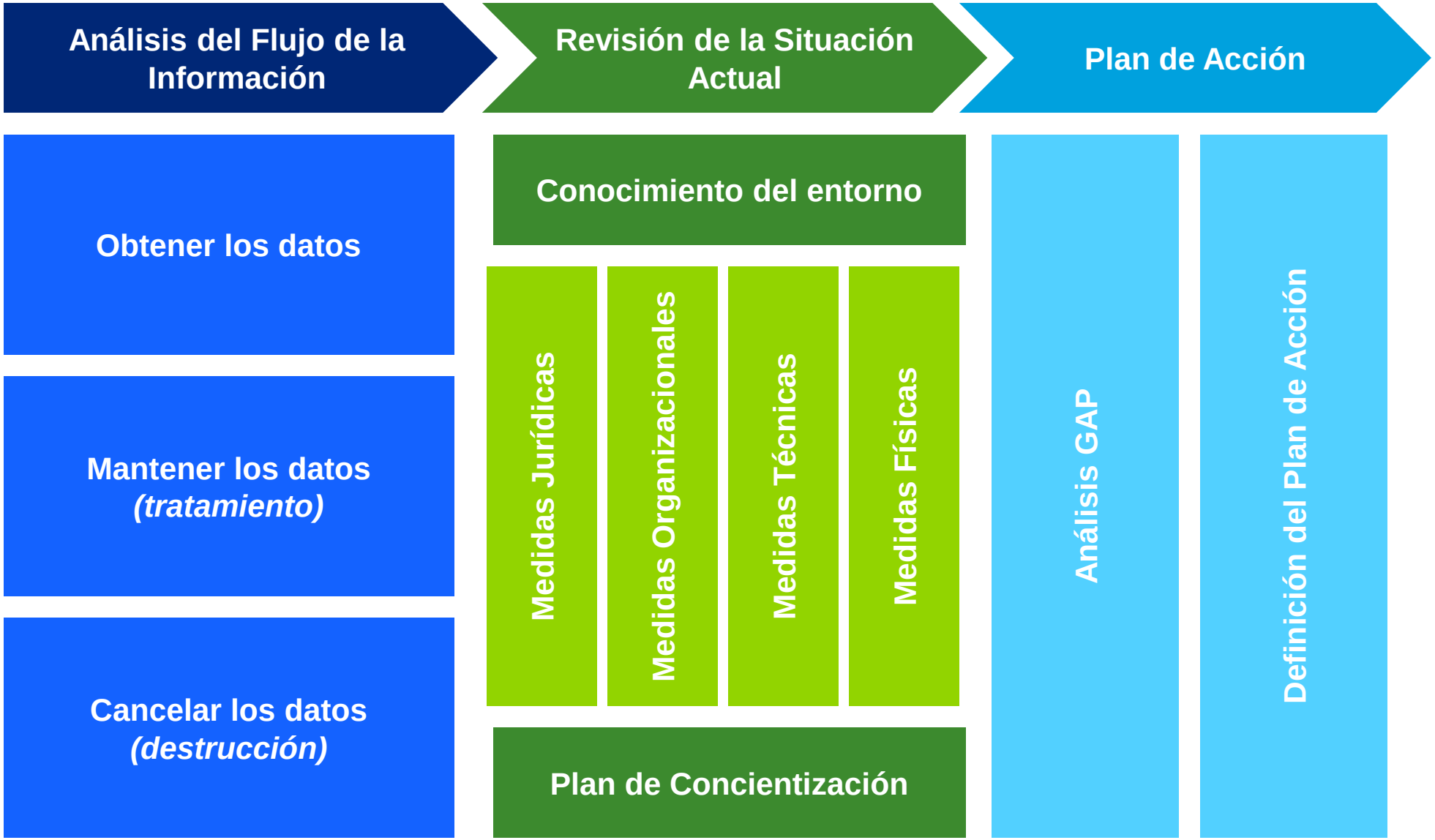
- Daños de la reputación / marca
- Incumplimiento regulatorio
- Costo de oportunidad
- Aumento en el nivel de atención y escrutinio
- Disminución de confianza de clientes, empleados, proveedores.

Tangibles

- Multas por incumplimiento
- Demandas
- Prisión (se contempla en la legislación mexicana)
- Pérdida de contratos
- Pérdida de productividad de empleados (reproceso)
- Requerimientos adicionales de seguridad y auditoría

¿Por dónde iniciar?

Primer paso, ¿Cómo estamos?



¿Preguntas?

Contactos

- **Eduardo Cocina Hernández, CISA, CGEIT**
  Socio
  Tel. 5080-6936
  ecocina@deloittemx.com

- **José González Saravia, CPA**
  Socio
  Tel. 5080-6722
  jgonzalezsaravia@deloittemx.com

- **Salomón Rico Baños, CISA, CISM, CGEIT**
  Socio
  Tel. 8133-7351
  srico@deloittemx.com

- **Miguel Ishii**
  Jones Day
  Tel. 30004000
  Mishii@jonesday.com

- **Alberto Durán Jacinto, CISA, CISM**
  Director
  Tel. 8133-7329
  aduran@deloittemx.com

- **Mayra Rivera Marchesini, CISA, CGEIT**
  Gerente
  Tel. 8133-7505
  mrivera@deloittemx.com

- **Oscar Mauricio Moreno López, CISSP, CISM, CISA**
  Gerente
  Tel. 5080-6569
  osmoreno@deloittemx.com

LFPDPPP

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

Sponsor / Dirección General
- Apoyo y definición de directrices requeridas para el cumplimiento de la LFPDP.

LFPDP
- Consta de 69 artículos, distribuidos en XI capítulos

Ley

Titulares
- Dueños de los Datos Personales.

Titulares

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

Solicitudes ARCO
Acceso
Rectificación
Cancelación
Oposición

Estándares Internacionales de Protección de Datos

Responsable

Obtener Datos
Consentimiento
Aviso de privacidad

Procesos

Sponsor/ Dirección General

Reglas

TI

Depto. Datos Personales

Legal

ifai

SECRETARÍA DE ECONOMÍA SE

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

Mantener Datos…
- ISO 27001
- DRP (BS25999)
- COBIT
- ISO 20001

Cancelar Datos

Reglamento
- 5 de Julio 2010
- 5 Julio 2011
- 5 Enero 2012

Terceros
- Entidades contratadas por el Responsable para el tratamiento de los datos personales (proveedores).
- Están sujetos a las mismas obligaciones que el Responsable.

Tercero

Mantener los Datos

Procesos de TI requeridos para el tratamiento de los datos:
- 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

Fechas Importantes
- 5 de julio 2010.- publicación de la Ley.
- 5 de julio 2011.- Designación del Depto. De Datos Personales. Avisos de Privacidad a Titulares.
- 5 de enero 2012.- Ejercicio de derechos ARCO. Inicia el procedimiento de protección de datos.