NYCE
Seguridad y Confianza

NYCE
PROTECCIÓN DE DATOS PERSONALES

Certificación de Protección de Datos Personales

www.nyce.org.mx

NYCE PROTECCIÓN DE DATOS PERSONALES

2054

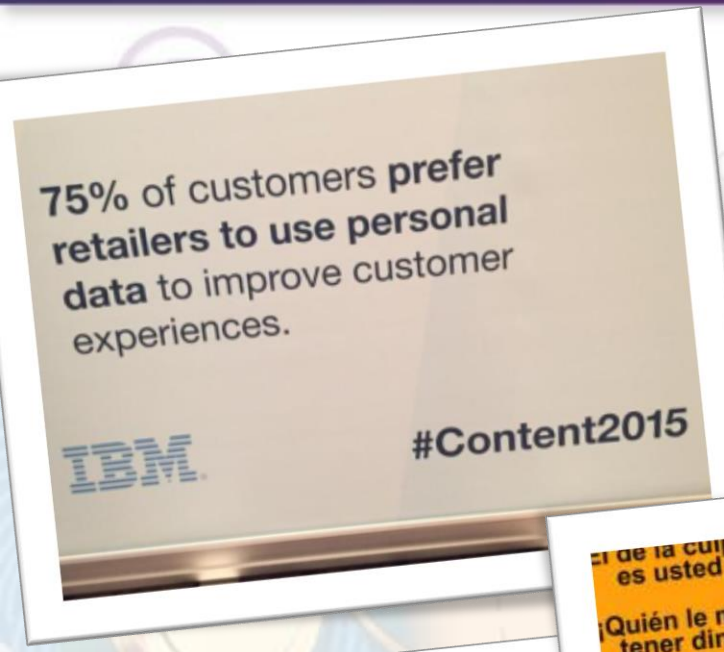
NYCE Seguridad y Confianza

Uso de datos personales e información sobre los usuarios

NYCE PROTECCIÓN DE DATOS PERSONALES

Por qué la protección de datos personales

NYCE Seguridad y Confianza



¿ Tu organización que datos personales trata ?

Nombre
Edad
Fecha de nacimiento
Estado civil
Hábitos
Teléfono
Trayectoria académica
Fotografía
Nacionalidad
E-mail
Religión

Nombre
E-mail
No. tarjeta
CVV

Nombre
E-mail
Ubicación
No. tarjeta
CVV
Celular

Nombre
E-mail
Ubicación
Frecuencia cardiaca

Nombre
E-mail
No. tarjeta
CVV

Nombre
Domicilio
E-mail
Teléfono
Estado de salud
No. tarjeta
CVV

Nombre
E-mail
Ubicación

¿Cuánto valen los datos personales?

Cuentas de juegos en Internet
12 a 3,500 US

Género
2.9 US

Passwords
76 US

Enviar spam
70 a 150 US

Tarjetas de crédito robadas
50 centavos- 20 US

Localización GPS
16 US

1,000 seguidores
2 a 12 US

Historial de crédito
30 US

Nombre
3.9 US

Historial de compra
20 US

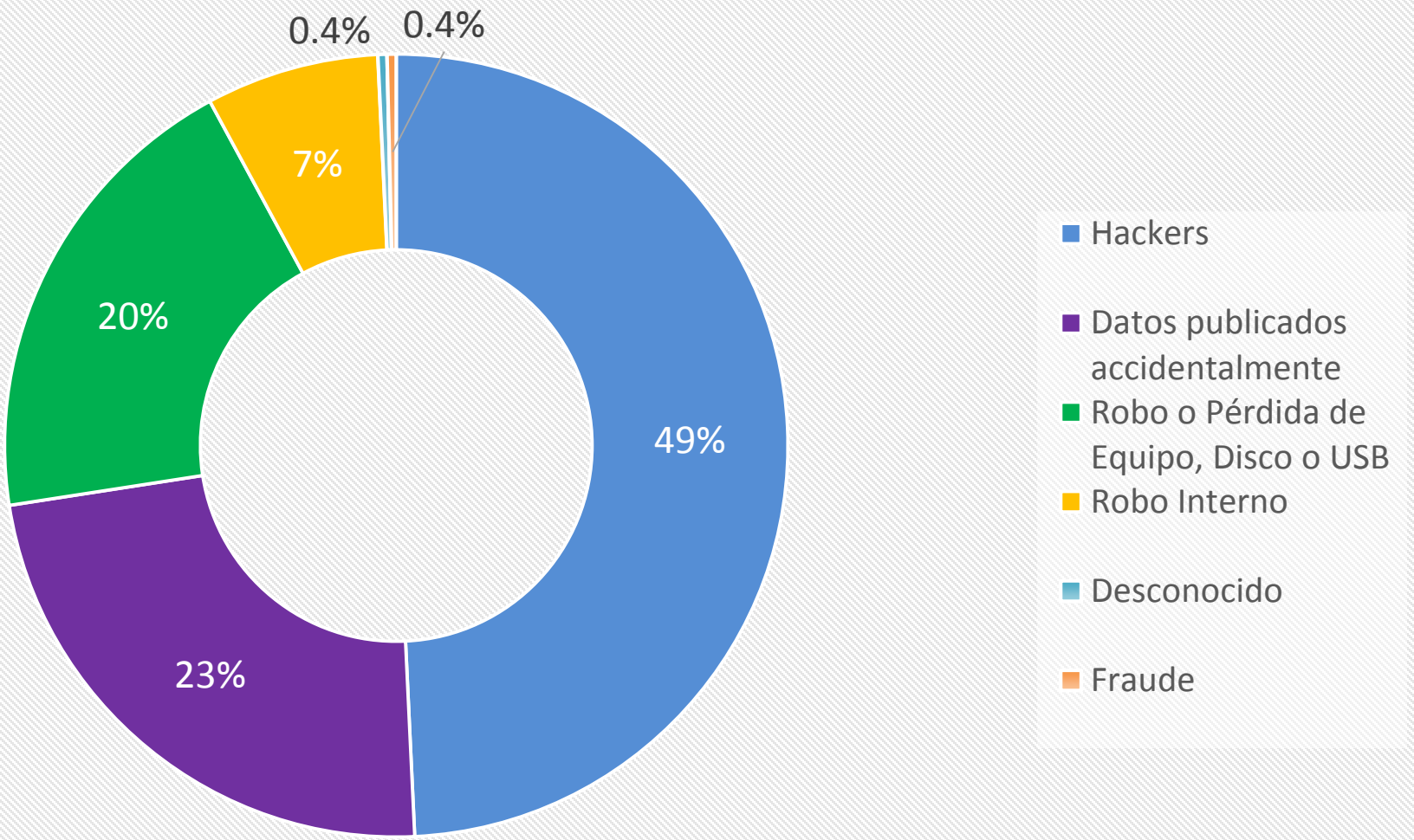
No. Teléfono
5.9 US

1,000 cuentas de correos electrónicos
10 US

Pasaportes reales escaneados
1 a 2 US

Fuente:
Ponemon Institute, Privacy and Security in a Connected Life, Marzo 2015 http://goo.gl/C5pj89
¿Cuánto cuestan los datos robados y servicios de ataque en el mercado clandestino? Symantec http://goo.gl/e41bec

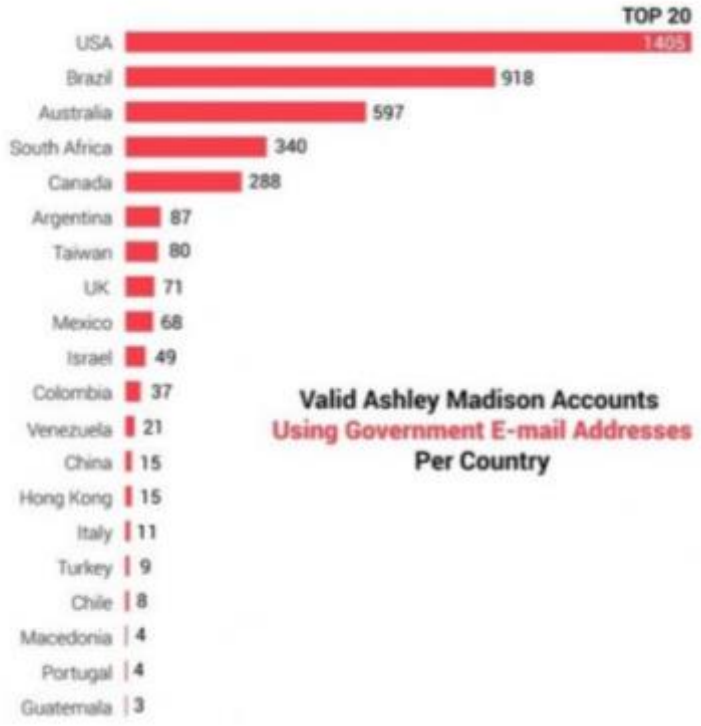
Principales causas de las fugas de datos



Importancia de los datos personales

33 millones de cuentas de personas usuarios del sitio

300 GB de datos



Nombre-dirección-teléfono-email-tarjeta de crédito

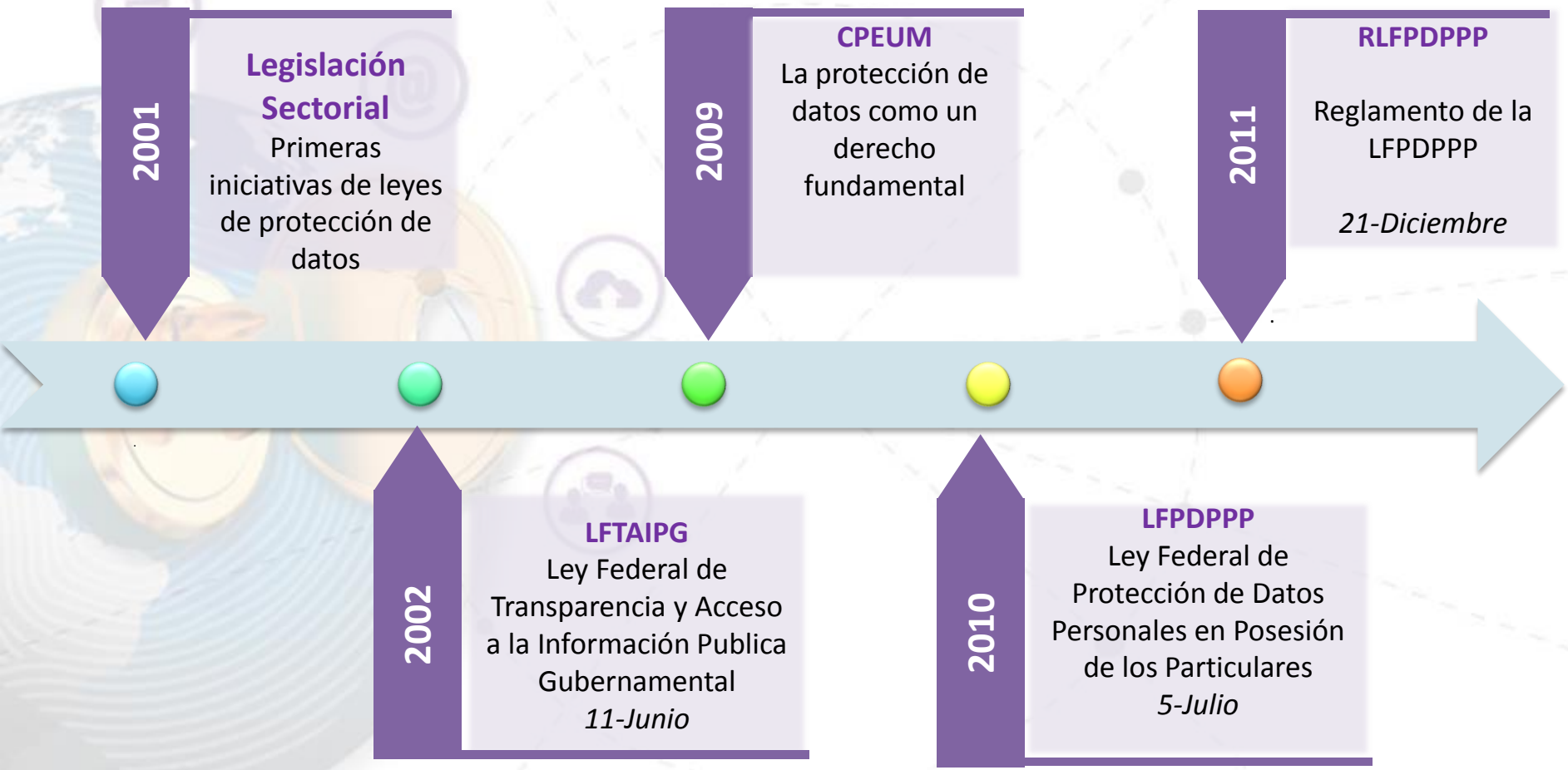
Extorsiones

Afectación a la vida personal

Daño a la reputación

SUICIDIO

Antecedentes en México



Marco legal y normativo

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley)

Reglamento de la LFPDPPP (Reglamento)

Lineamientos del aviso de privacidad (lineamientos)

- Recomendaciones de Seguridad (recomendaciones)
- Recomendaciones para la designación de la persona o Departamento de Datos Personales
- Guía para implementar un SGSDP
- Parámetros de autorregulación en materia de protección de datos personales
- Guía para cumplir con los principios y deberes de la LFPDPPP

De la Ley

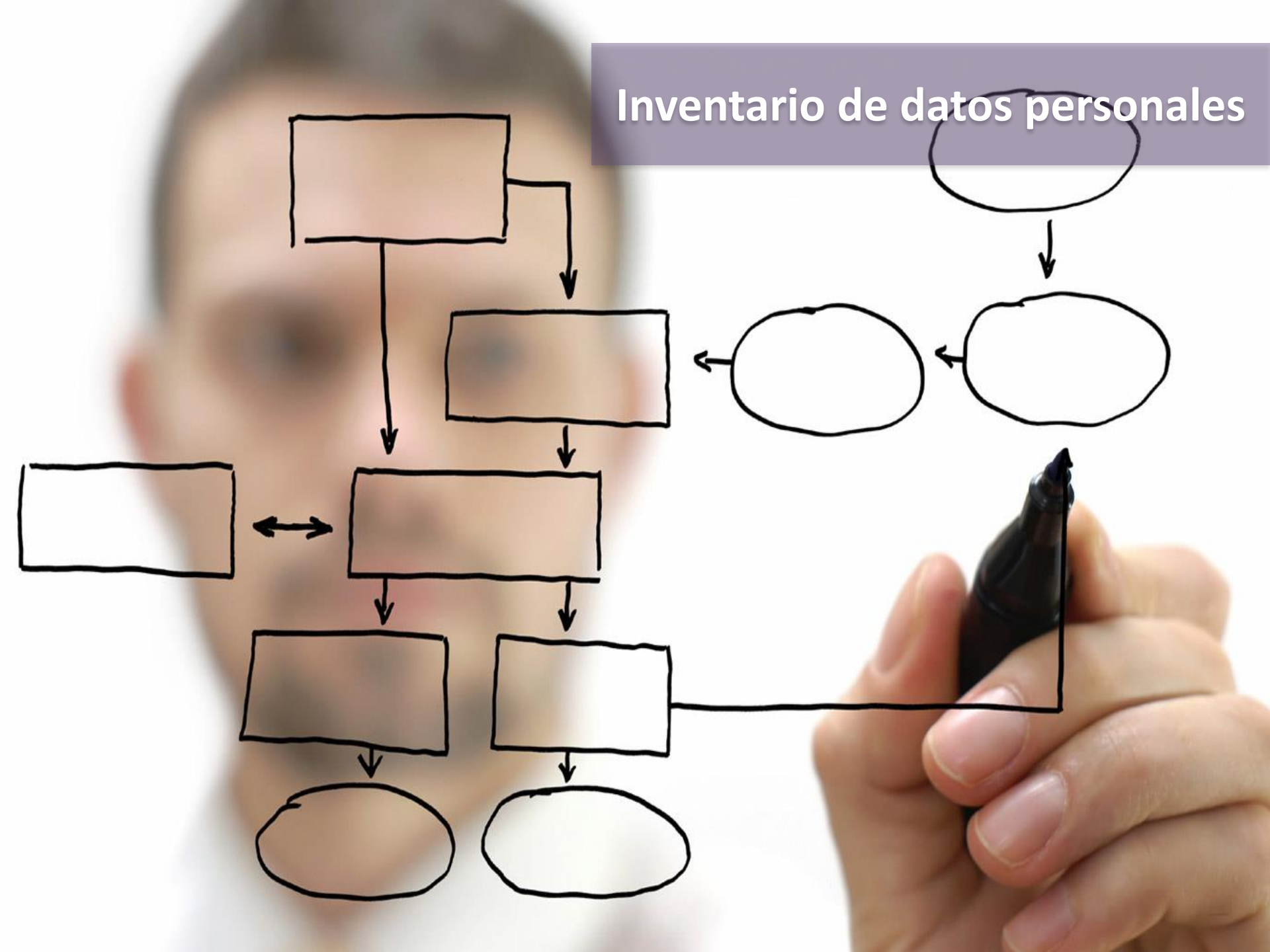
La LFPDPPP

"Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la **protección de los datos personales** en posesión de los particulares, 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."

Lo mínimo ….


Aviso de privacidad
Procedimientos para atención de derechos ARCO
Designación de responsable o departamento al interior
Políticas de Seguridad y protección de datos
Convenios de confidencialidad y contratos
Acciones y procedimientos en caso de vulneración
Capacitar al personal involucrado
Inventario de Datos personales y sistemas de tratamiento
Identificación de personas que tratan los datos, privilegios, roles y responsabilidades
Análisis de riesgos
Análisis de brecha
Datos
Finalidades
Tratamientos
Consentimiento Tácito - Expreso
Privilegios de Acceso y transferencias
Identificar
¿Para qué?
¿Qué voy a hacer con ellos?
Evidencia
Internos
Externos
Medidas de seguridad Administrativas
Medidas de seguridad Físicas
Medidas de seguridad Técnicas

Inventario de datos personales



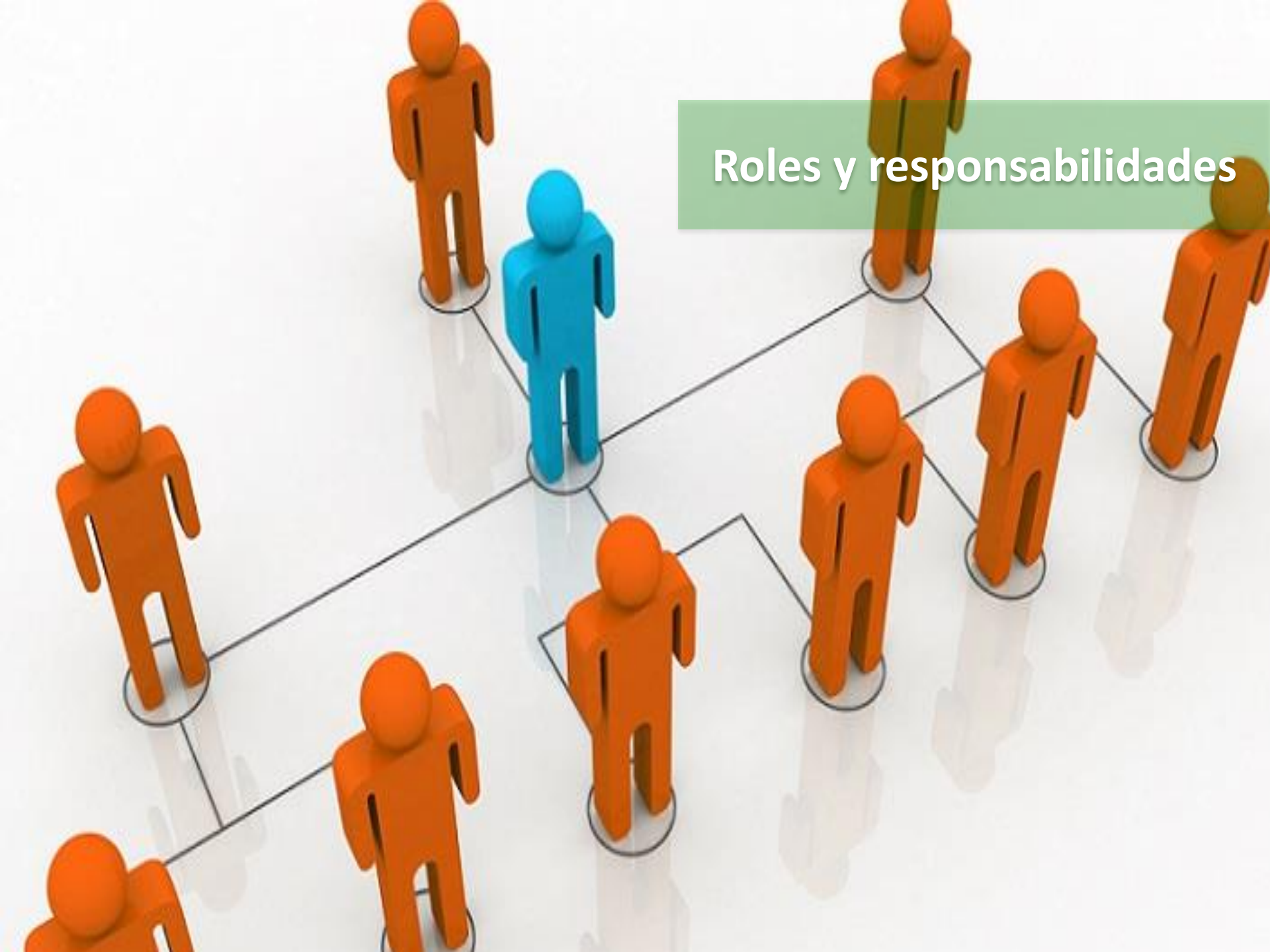
¿A quién debo involucrar en mi organización?

"involucrar a todas las áreas que manejen los datos"

Ciclo de vida de los datos personales

Tratamiento de DP por Internos / Externos

Roles y responsabilidades



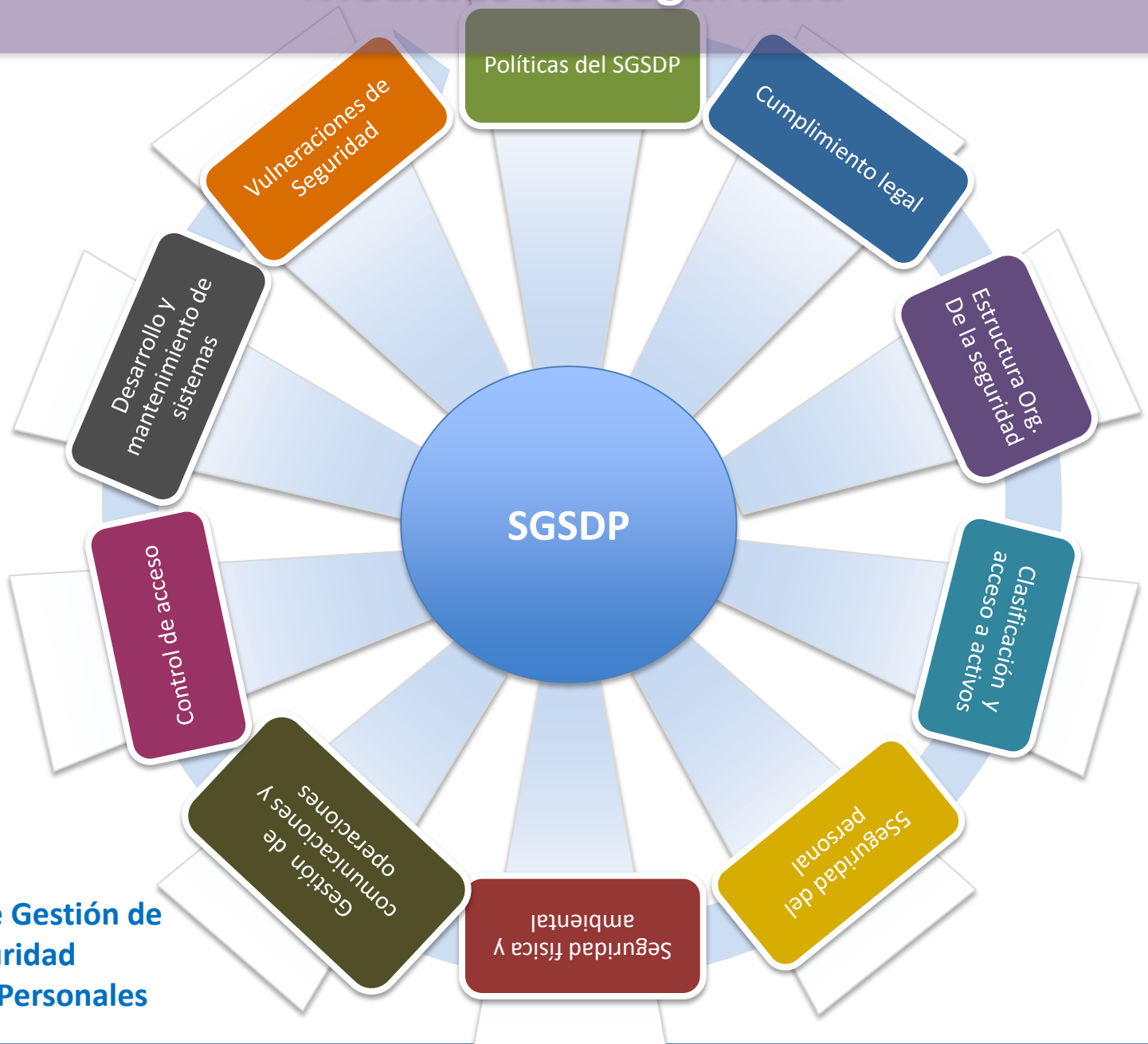
Análisis de riesgos y Análisis de brecha

Análisis de riesgos

La clave

- El **valor** de los datos personales para los titulares.
- La **exposición** de los activos involucrados con los datos personales
- El **valor potencial para un atacante** o tercera persona no autorizada para la posesión de los datos personales
- La **trazabilidad** y posibilidad de identificar quién tuvo acceso a los datos personales.

Medidas de seguridad



Sistema de Gestión de Seguridad de Datos Personales

De la Ley

La LFPDPPP en su Art. 19 establece que:

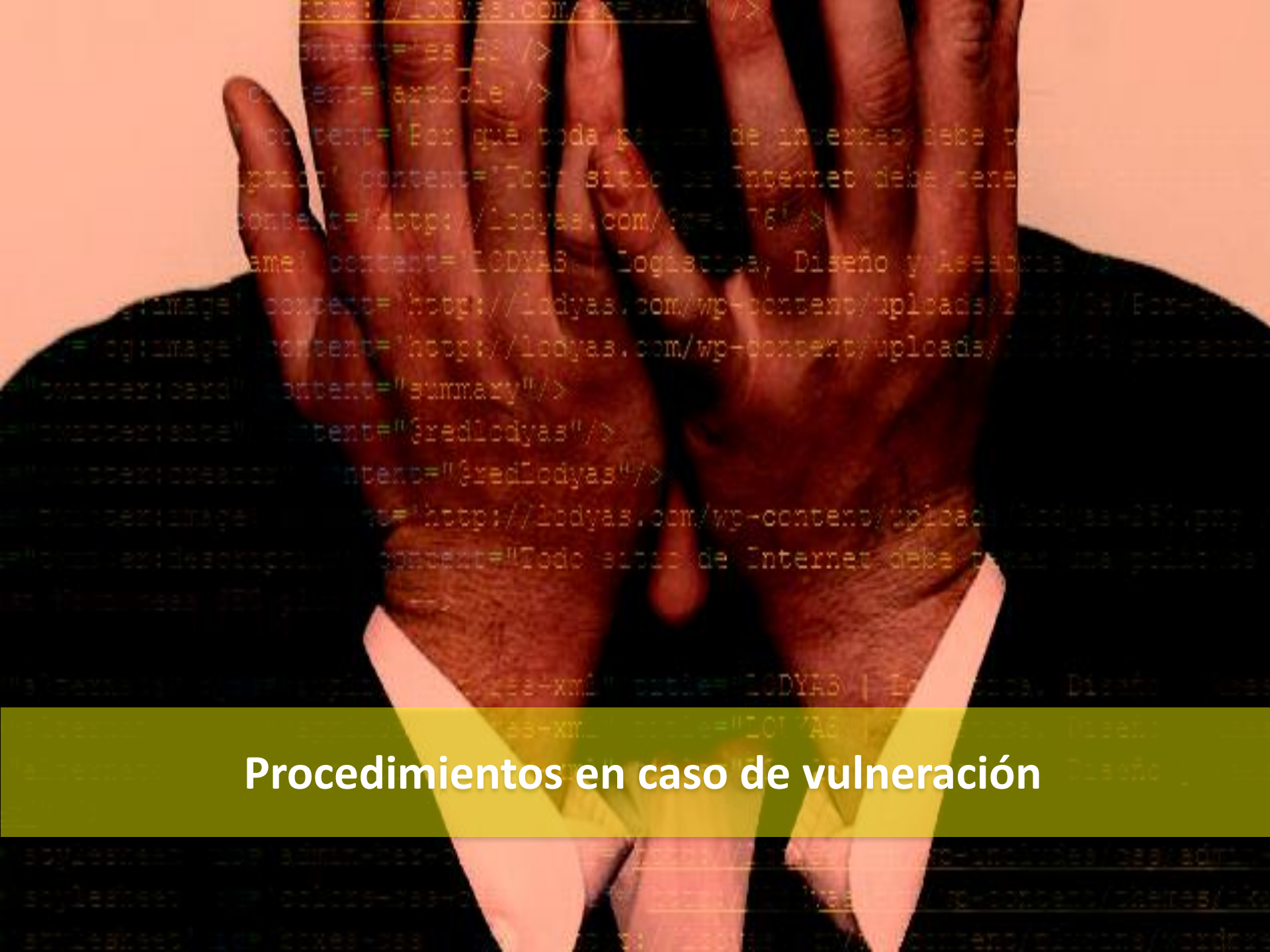
"Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad **administrativas**, **técnicas** y **físicas** que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables **no adoptarán medidas de seguridad menores a aquéllas que mantengan para el manejo de su información**. Asimismo se tomará en cuenta el riesgo existente, las posibles **consecuencias para los titulares**, la **sensibilidad de los datos** y el **desarrollo tecnológico**."

Designación responsable al interior de la protección de datos personales

Política de datos personales

Convenios de confidencialidad y contratos con terceros



Procedimientos en caso de vulneración

Vulneraciones

Reglamento LFPDPPP Artículo 63.

Notificación de vulneraciones de seguridad

Deberá informarse a los titulares involucrados en la vulneración:

Artículo 65 del Reglamento de la LFPDPPP

1. La naturaleza de la vulneración
2. Los datos personales comprometidos
3. Recomendaciones al titular para proteger sus intereses
4. Las acciones correctivas realizadas de forma inmediata
5. Los medios donde se puede obtener más información al respecto

Capacitación y concientización

Derechos ARCO

Acceso

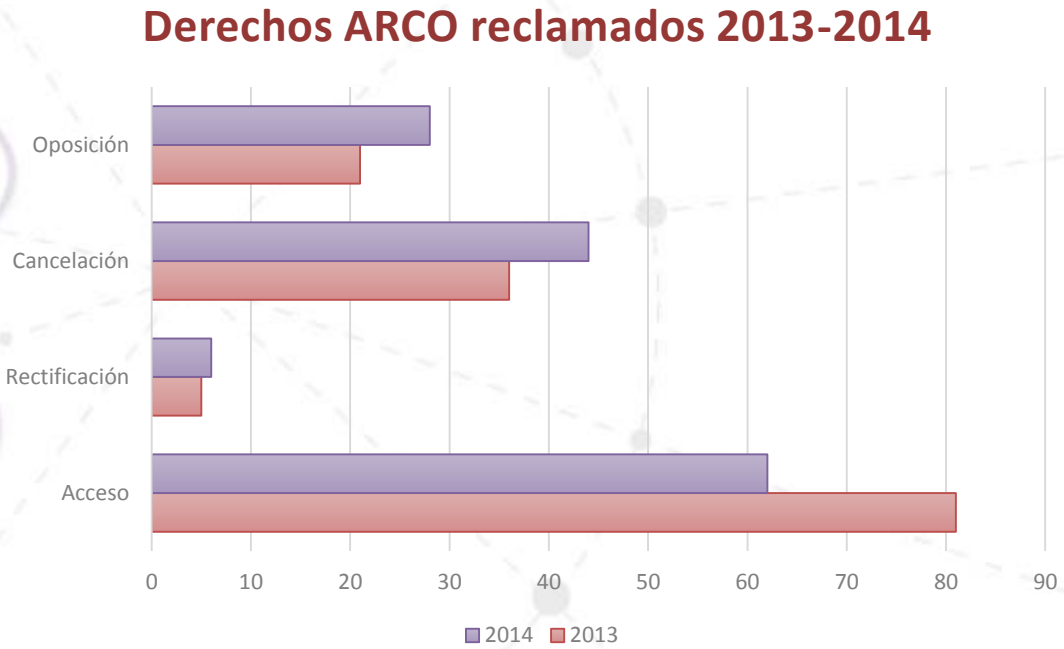
Rectificación

Cancelación

Oposición

Derechos ARCO

- Derechos arco
  - Acceso
  - Rectificación
  - Cancelación
  - Oposición



Fuente: Elaboración propia con información de Informe de labores 2014,INAI

Avisos de privacidad

Estructura

El Aviso de Privacidad debe contener:

- Datos del responsable
- Las finalidades del tratamiento de datos (y si se recaban o no datos sensibles)
- Las opciones y medios para limitar el uso o divulgación de los datos
- Los medios para ejercer los derechos ARCO
- En su caso, las transferencias de datos que se efectúen
- El procedimiento y medio por el cual el responsable comunicará a los titulares los cambios al aviso de privacidad

Infracciones y sanciones

Apercibimiento

Incumplir solicitudes ARCO

100-160mil DSMGVDF

- Negligencia o dolo en trámites ARCO
- Declarar dolosamente inexistencia
- Incumplimiento de principios de Ley
- Omisiones en aviso de privacidad
- Datos inexactos
- Incumplimiento de apercibimiento

200-320mil DSMGVDF

- Incumplimiento de deber de confidencialidad
- Uso desapegado a la finalidad marcada en Aviso
- Transferir datos sin comunicar aviso de privacidad
- Vulneración a la seguridad
- Transferir sin consentimiento del titular
- Obstruir verificación de autoridad
- Transferencia o cesión en contra de Ley
- Recabar datos en forma engañosa o fraudulenta
- Uso ilegítimo de datos en caso de solicitud de cese
- Impedir ejercicio derechos ARCO
- No justificar tratamiento de datos sensibles

Las sanciones pueden duplicarse en caso de

Datos Sensibles

Reincidencia

El INAI considerará:
Naturaleza del dato (sensibles, financieros y patrimoniales)
Negativa injustificada del Responsable a solicitudes del Titular
Intencionalidad en la infracción
Capacidad económica
Reincidencia

Delitos:

- 3 meses a 3 años de prisión – con ánimo de lucro, vulnerar seguridad a bases de datos
- 6 meses a 5 años de prisión – con ánimo de lucro indebido, tratar datos personales mediante engaño o error

LFPDPPP Capítulo X y XI Artículo 63 al 69

Algunas sanciones impuestas:

OCEANICA:

- INAI solicitó en dos ocasiones un informe relacionado con la publicación, que reveló que Oceánica había **dejado al descubierto los datos de una persona que había sido paciente en sus instalaciones** pero Oceánica **no atendió** ninguno de ellos. Por esta omisión, el IFAI ordenó una visita de verificación.
- Cuando el personal del Instituto se presentó al domicilio de Operadora Oceánica Internacional en Mazatlán Sinaloa, no le dieron las facilidades correspondientes y personal de esta institución le **negó el acceso al inmueble**, obstruyendo con ello los actos de verificación de la autoridad.
- Oceánica promovió un juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa, autoridad que el 8 de abril de 2013 dictó sentencia definitiva en contra de esta empresa.
- Imponiéndole **una multa de $2,493,200 pesos**,

Algunas sanciones impuestas (cont.):

Pharma Plus, S.A. de C.V. (Farmacias San Pablo)

- INAI impuso dos multas a Pharma Plus por un total de **$2,000,045.04 pesos**:
  - $1,500,033.78 **por no proporcionar información sobre el tratamiento a que serían sometidos los datos personales** que recaba de sus clientes (contraviniendo el principio de información).
  - $500,011.26 por **omitir el elemento de identidad en su aviso de privacidad** (aparecía nombre comercial en lugar de razón social).

Algunas sanciones impuestas (cont.):

Sport City, S.A. de C.V.

- INAI impuso una multa a Sport City por un total de **$1,246,600.00 pesos**:
  - Por **omitir algunos de los elementos del Aviso de Privacidad** (no señaló a través de qué medios los titulares de los datos podrán limitar el uso o divulgación de sus datos).

Algunas sanciones impuestas (cont.):

Caja Popular Cristo Rey, S.C. de R.L. de C.V.

- INAI impuso a Caja Popular Cristo Rey tres multas por un total de: **$2,181,550.00 pesos**:
  - $545,387.50 pesos por **no poner a disposición de los titulares el Aviso de Privacidad.**
  - $779,125.00 pesos por no recabar el consentimiento para el tratamiento de datos financieros.
  - $857,037.50 pesos por no contar con una persona o departamento de privacidad, ni con un procedimiento para dar atención a las solicitudes de derechos ARCO.

Algunas sanciones impuestas (cont.):

Banco Nacional de México, S.A

- INAI impuso cinco multas a BANAMEX por un total de **$16,155,936.00 pesos**:
  - $2,493,200.00 pesos porque Banamex fue **negligente en el trámite de la solicitud de cancelación y oposición** que le había presentado el titular de los datos.
  - $1,196,736.00 porque Banamex **continuó tratando los datos cuando el fin por el cual fueron recabados se había agotado**.
  - $2,493,200.00 por **no efectuar la cancelación** de los datos cuando la misma resultaba procedente.
  - $4,986,400.00 pesos por **continuar en el tratamiento ilegítimo** de los datos del titular.
  - $4'986,400.00 pesos porque Banamex **impidió el ejercicio de los derechos de cancelación y oposición del titular.**
- Banamex impugnó la Resolución del INAI en el TFJFA y obtuvo una suspensión provisional

Algunas sanciones impuestas (cont.):

Banco Nacional de México, S.A.

- INAI impuso multa a BANAMEX por: **2,493,200.00** por **falta de respuesta a una solicitud de ejercicio de derechos ARCO** (escrito libre y no un formato prediseñado por Banamex) y no comparecer al procedimiento de protección de derechos en el IFAI

Algunas sanciones impuestas (cont.):

TARJETAS BANAMEX (SOFOM ER)

Banamex

- INAI impuso cuatro multas a BANAMEX por un total de **$9,848,140.00 pesos**:
  - $1,495,920.00 pesos porque **por obstruir los actos de verificación** de la autoridad al negarse de manera reiterada a proporcionar la información y documentación requerida sin justificación legal.
  - $1,246,600.00 **por mantener datos inexactos del Titular** y no efectuar acciones para la rectificación o cancelación de los mismos. (gestión de cobranza por encargado con datos equivocados)
  - $3,490,480.00 por **continuar con el uso ilegítimo de los datos personales** del Titular, a pesar de que este solicito que fueran rectificados y cancelados.
  - $3,615,140.00 pesos **por violación a los principios** de consentimiento, calidad y responsabilidad

Algunas sanciones impuestas (cont.):

MÉDICO PARTICULAR

- Multa impuesta por el INAI a un médico por **$41,874.00** pesos, **por haber transferido datos personales sensibles** de alguno de sus pacientes, **sin contar con el consentimiento del titular**, y por **no haber señalado expresamente en su Aviso de Privacidad las opciones y medios que ofrecía para limitar el uso o divulgación de los mismos**.

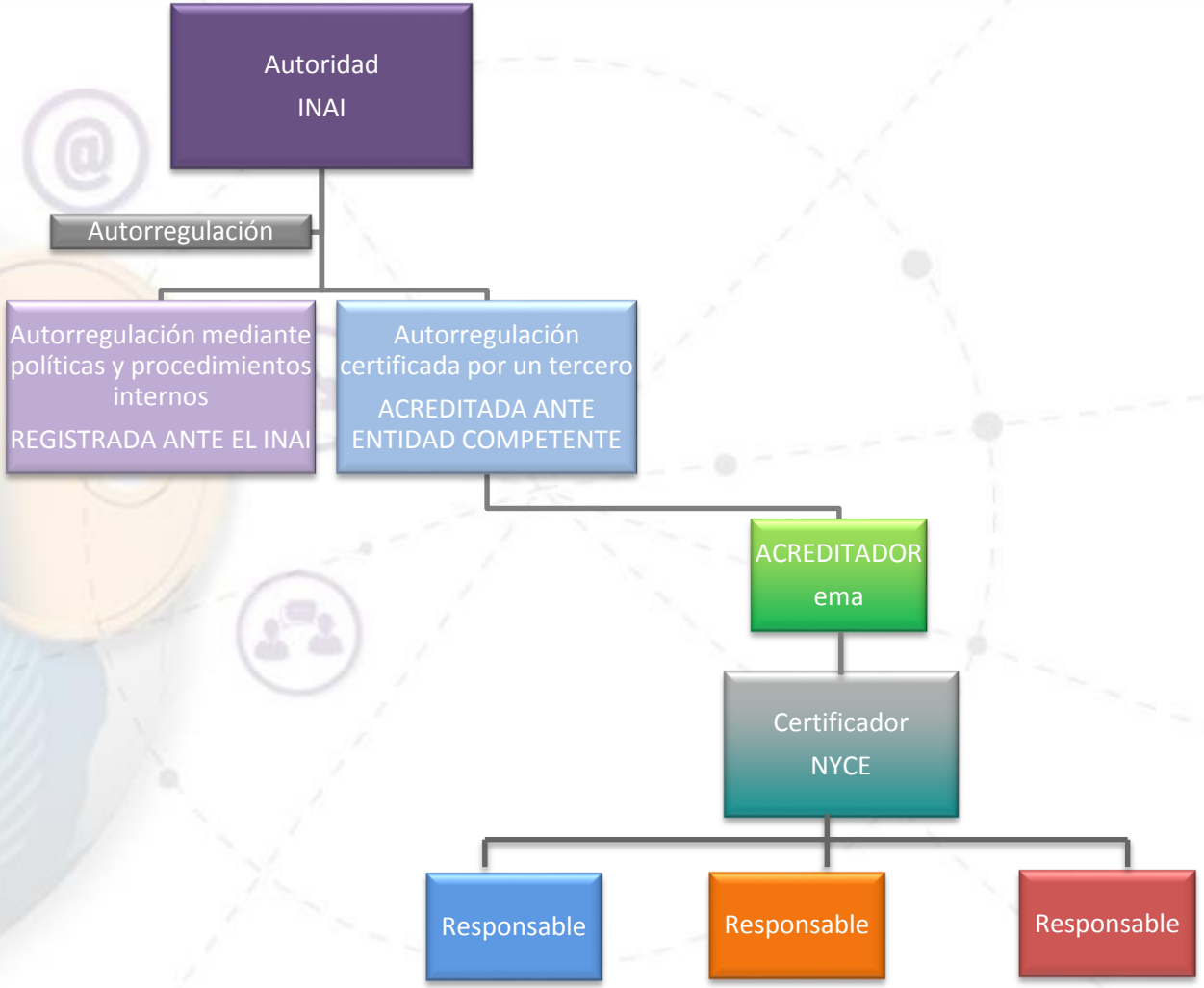
Esquema de Autorregulación Vinculante

Marco Legal

LFPDPPP	RLFPDPPP	Parámetros de Autorregulación en Materia de Datos Personales
5 Julio 2010 Artículo 44	21 Diciembre 2011 Artículos 47, 79-86,	29 Mayo 2014 Artículos 13-37,

Esquema de autorregulación vinculante o esquema: Conjunto de principios, normas y procedimientos, de adopción voluntaria y cumplimiento vinculante, que tiene como finalidad regular el comportamiento de los responsables y encargados respecto a los tratamientos de datos personales que lleven a cabo

Autorregulación Vinculante

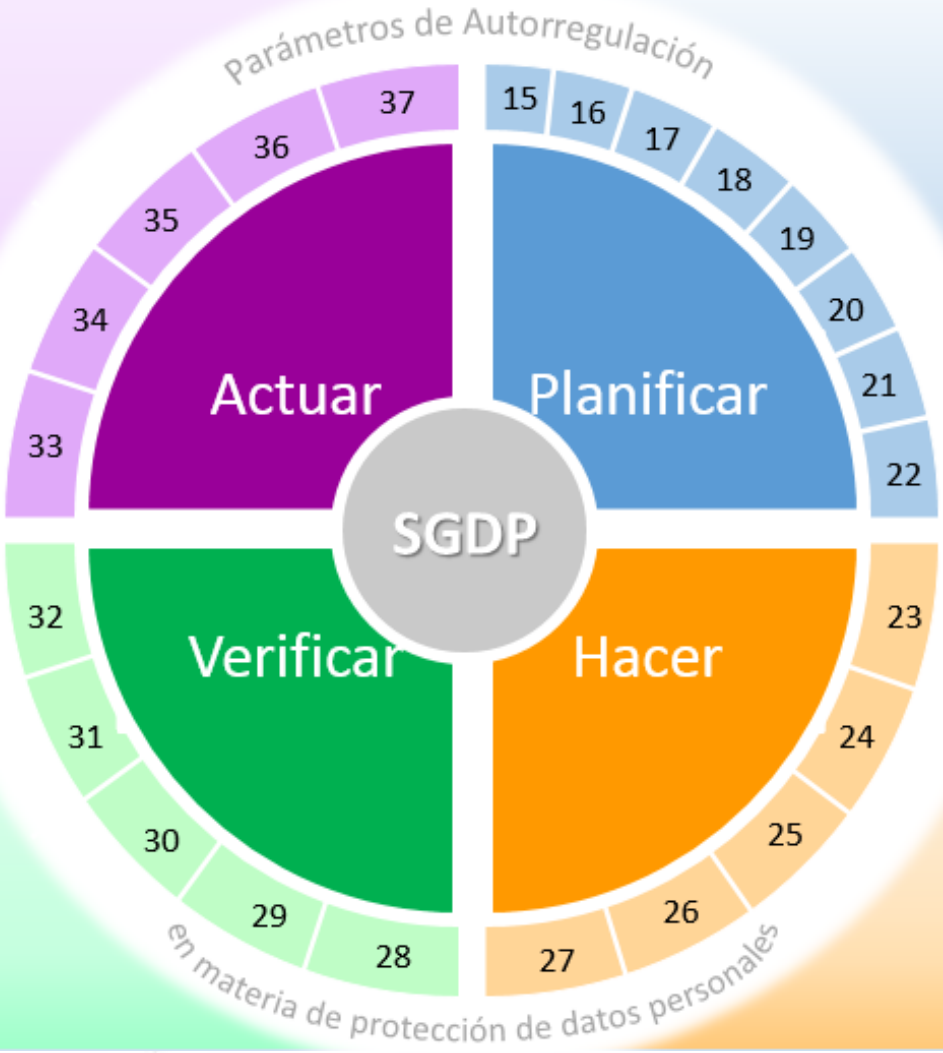


El Instituto comenta …

Sistema de Gestión de Datos Personales

Acciones
- Preventivas
- Correctivas

Mejora continua



Objetivos
Alcance
Política datos personales
Apoyo alta dirección
Responsable
Funciones/responsabilidades
Recursos

Actualizar el SGDP
Auditoría
Revisión administrativa

Capacitación /cultura
Inventario datos personales
Análisis de riesgos y brecha
Procedimientos
- Controles
- Contratos
- Aviso de privacidad
- Vulneraciones

Para todos los sectores

Industria Comercio y servicios

- Call centers y contact centers
- Agencias de viajes
- Tiendas departamentales
- Clubes deportivos
- Entretenimiento

Salud

- Hospitales
- Clínicas
- Cadenas de farmacias
- Laboratorios
- Servicios funerarios

Financiero

- Bancos
- Seguros
- Afores
- Casas de bolsa

Educación

- Escuelas
- Universidades
- Centros de capacitación
- Centros de Idiomas

Telecomunicaciones

- ISP
- **Telefonía**
- **Servicios de suscripción**

Cámaras y asociaciones

Beneficios

Confianza de parte de los consumidores de productos o servicios

Prestigio al ostentar una certificación con validez internacional

Apego a **estándares y normas internacionales**

Adopción voluntaria del esquema

Atenuación de sanciones

Demostración de cumplimiento ante la autoridad

GRACIAS

M.A. Miriam PADILLA ESPINOSA

Subgerente Certificación de Protección de Datos Personales

Normalización y Certificación Electrónica S.C.

1204 5191 ext 417

mpadilla@nyce.org.mx

@Ing_Mili