CAPACITACIÓN

Ley y lineamientos en materia de protección de datos personales en posesión de sujetos obligados del Estado de Puebla Pt. II.

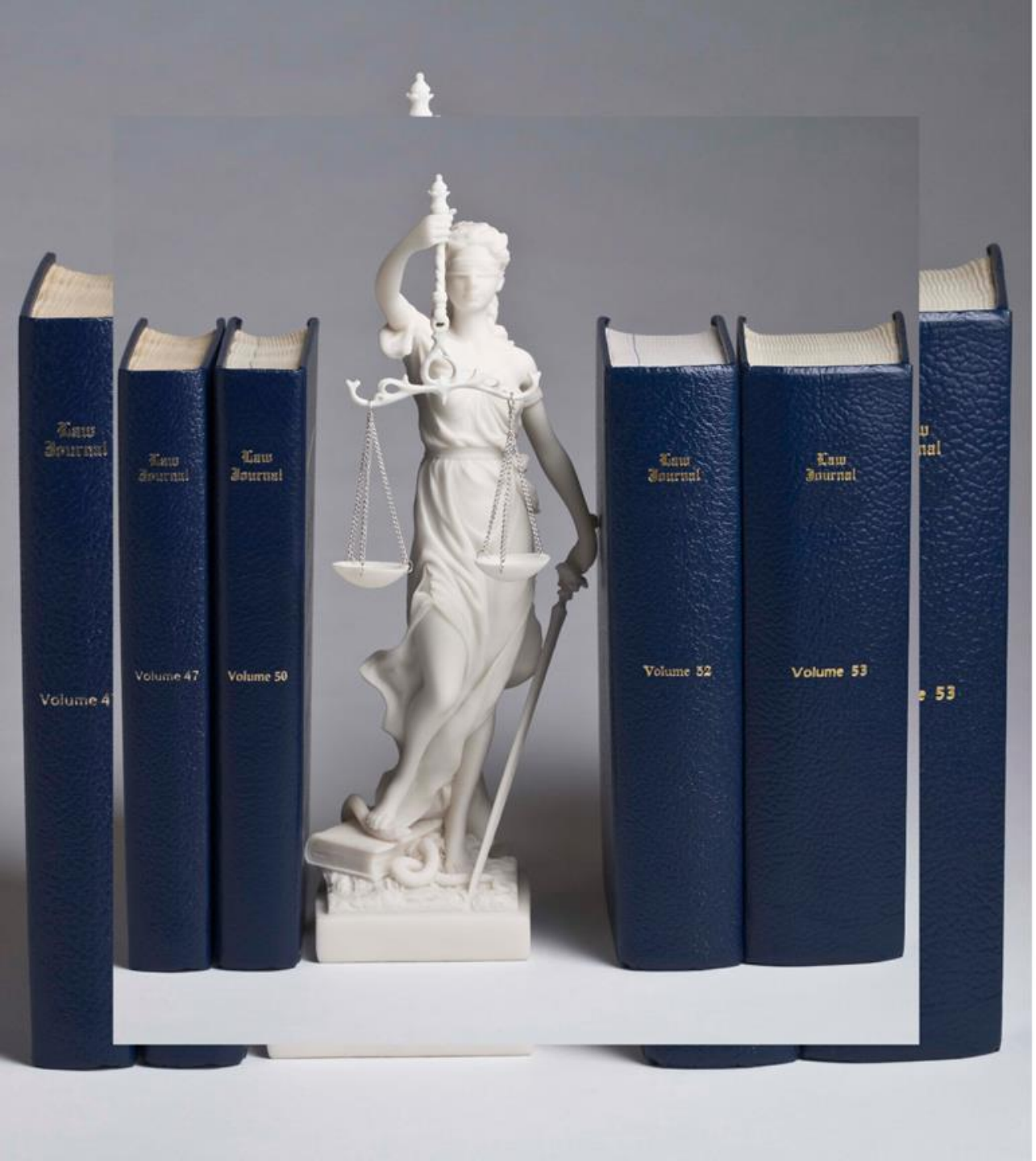
ITAIPUE

CONTENIDO

- **Antecedentes**
    - Origen
    - Evolución
    - Definición
- **Ejercicio de Derechos ARCO**
    - Acceso
    - Rectificación
    - Cancelación
    - Oposición
    - Portabilidad
- Principios del tratamiento de Datos Personales
    - Licitud
    - Finalidad
    - Lealtad
    - Consentimiento
    - Calidad
    - Proporcionalidad
    - Información
    - Responsabilidad
- Deberes
    - De Seguridad
    - De Confidencialidad

CONTENIDO

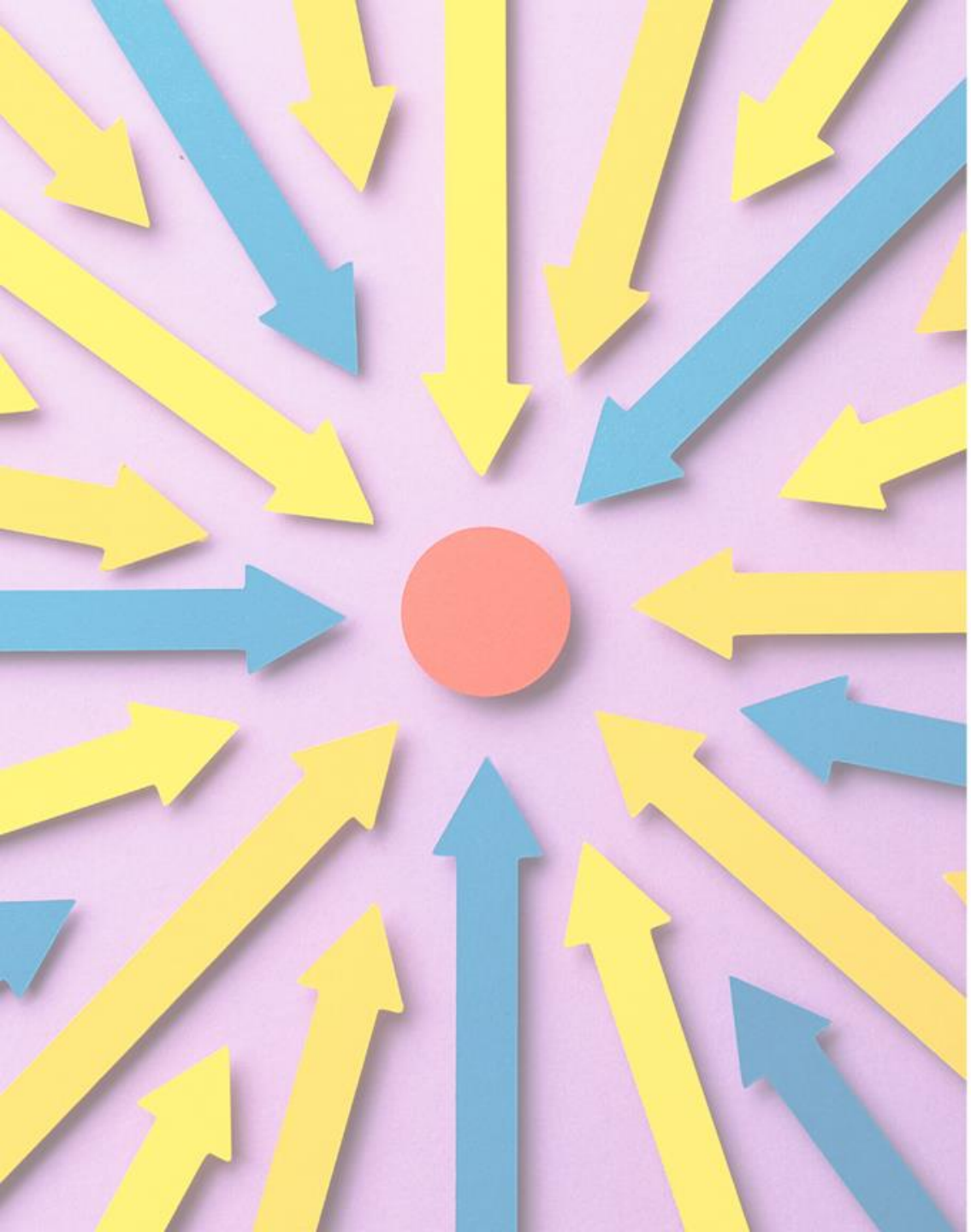
- Antecedentes
    - Origen
    - Evolución
    - Definición
- Ejercicio de Derechos ARCO
    - Acceso
    - Rectificación
    - Cancelación
    - Oposición
    - Portabilidad
- **Principios del tratamiento de Datos Personales**
    - Licitud
    - Finalidad
    - Lealtad
    - Consentimiento
    - Calidad
    - Proporcionalidad
    - Información
    - Responsabilidad
- Deberes
    - De Seguridad
    - De Confidencialidad



LICITUD

El responsable deberá:

- Tratar los datos personales con **estricto apego y cumplimiento de** lo dispuesto por **la ley**, y
- Sujetarse a las **facultades o atribuciones** que la normativa aplicable le confiera.



FINALIDAD

El tratamiento de datos personales deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas.

Las finalidades son:

I. **Concretas:** cuando el tratamiento de datos personales atiende a la consecución de fines específicos o determinados (no genéricos);
II. **Explícitas:** cuando se expresan y dan a conocer de manera clara en el aviso de privacidad;
III. **Lícitas y legítimas:** cuando son acordes con las atribuciones expresas del responsable y con la ley.

PRINCIPIOS DEL TRATAMIENTO

LEALTAD

El responsable deberá **abstenerse** de tratar los datos personales a través de **medios engañosos o fraudulentos**; además, deberá **privilegiar** la **expectativa razonable de protección de datos personales**.

CONSENTIMIENTO

El responsable deberá obtener el consentimiento del titular para el tratamiento de sus datos personales, salvo que se actualice alguna de las siguientes causales de excepción:

1. Cuando una **norma con rango de ley** expresamente lo permita;
2. Cuando exista **resolución** por parte **de autoridad competente**;
3. Cuando los datos sean necesarios para el **reconocimiento o defensa de derechos** del titular ante autoridad competente;
4. Cuando los datos se requieran para **ejercer un derecho o cumplir con obligaciones derivadas de una relación jurídica** entre el titular y el responsable;
5. Cuando exista una **situación de emergencia** que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
6. Cuando los datos sean necesarios para la prevención, el diagnóstico médico, la **prestación de asistencia sanitaria**, tratamiento médico o gestión de servicios sanitarios;
7. Cuando los datos figuren en **fuentes de acceso público**.

PRINCIPIOS DEL TRATAMIENTO

El consentimiento debe ser:

1) **Libre:** debe prestarse sin error, coacción, violencia, dolo o mala fe.
2) **Específico:** debe prestarse en relación a finalidades concretas y no generales.
3) **Informado:** debe prestarse con conocimiento de los términos del respectivo aviso de privacidad.

El consentimiento puede ser:

Expreso: cuando se recaben datos personales sensibles. Este tipo de consentimiento se puede manifestar de forma verbal, por escrito, por medios electrónicos, o cualquier otra tecnología que fehacientemente identifique la identidad del titular y permita al responsable probar su obtención.

En caso de consentimiento expreso por escrito, bastará un documento firmado o con huella dactilar. En caso de consentimiento expreso por medios electrónicos, podrá emplearse la firma electrónica.

En cualquier caso, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual manifestar su consentimiento expreso.

Tácito: cuando, habiéndose puesto a disposición del titular el respectivo aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

REGLA GENERAL → Consentimiento tácito, salvo que una ley exija que la voluntad del titular se manifieste de forma expresa.

PRINCIPIOS DEL TRATAMIENTO

CALIDAD

Es el deber a cargo del responsable de adoptar medidas necesarias para mantener **exactos, correctos y actualizados** los datos personales que se encuentren en su posesión.

TEMPORALIDAD

El responsable deberá suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades del tratamiento, previo bloqueo, en su caso, y una vez concluidos los plazos de conservación.

El responsable deberá establecer procedimientos para la **conservación, bloqueo y supresión** de los datos personales en su posesión. En la determinación de dichos plazos, el responsable deberá considerar los valores administrativos, contables, fiscales, jurídicos e históricos de los datos personales, así como atender las disposiciones aplicables en la materia de que se trate.

PRINCIPIOS DEL TRATAMIENTO

BLOQUEO

Conservación de los datos personales, una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con el tratamiento, hasta el plazo de prescripción legal o contractual.

Durante dicho periodo, los datos personales se conservan pero sin aprovechamiento.

Transcurridos esos plazos de conservación, los datos personales deben ser suprimidos definitivamente.

PROPORCIONALIDAD

Exige que cualquier tratamiento de datos personales no vaya más allá de lo necesario para alcanzar sus objetivos.

Este deber se traduce en que los datos personales que se pretendan recabar del titular sean adecuados, relevantes, pertinentes y **estrictamente necesarios** para la finalidad que justifica su tratamiento.

Criterio de minimización

PRINCIPIOS DEL TRATAMIENTO

INFORMACIÓN

El responsable debe informar al titular, a través del aviso de privacidad, la **existencia**, los **alcances**, los **términos** y las **condiciones** del tratamiento al que serán sometidos sus datos personales.

Existen dos modalidades de aviso de privacidad en el sector público:

AVISO SIMPLIFICADO

I. Denominación del responsable.
II. Finalidad del tratamiento:
   - ✓ Ser específicos y claros en la redacción (evitar generalidades, redacción confusa, empleo de frases inexactas, ambiguas o vagas como "entre otras finalidades", "para fines análogos", "por ejemplo", etc.
   - ✓ Hay que distinguir aquellas finalidades que sí requieren consentimiento de aquellas otras que no lo requieren.
III. Indicar las posibles transferencias a que haya lugar y que requieran de consentimiento, señalando destinatarios y finalidades de las mismas.
IV. Mecanismos y medios para que el titular pueda manifestar su negativa para finalidades y transferencias que requieran de su consentimiento.
V. Sitio donde consultar el aviso de privacidad integral.

AVISO INTEGRAL

I. Domicilio del responsable.
II. Datos personales.
III. Fundamento legal que faculta al responsable a llevar a cabo el tratamiento y las transferencias de datos personales.
IV. Mecanismos, medios y procedimientos para el ejercicio de derechos ARCO.
V. Domicilio de la Unidad de Transparencia.
VI. Medios de comunicación de los cambios al aviso de privacidad y fecha de elaboración o, en su caso, de última actualización.

RESPONSABILIDAD

I. Destinar **recursos** para elaboración de políticas y programas;
II. Elaborar **políticas y programas**;
III. Llevar a cabo un programa de **capacitación**;
IV. R**evisar periódicamente** esas políticas y programas;
V. Establecer un sistema de **vigilancia** para comprobar el cumplimiento de esas políticas y programas;
VI. Establecer procedimientos para la atención de **dudas y quejas** por parte de los titulares;
VII. Privacidad por **diseño**;
VIII. Privacidad por **defecto**.

CONTENIDO

- Antecedentes
    - Origen
    - Evolución
    - Definición
- Ejercicio de Derechos ARCO
    - Acceso
    - Rectificación
    - Cancelación
    - Oposición
    - Portabilidad
- Principios del tratamiento de Datos Personales
    - Licitud
    - Finalidad
    - Lealtad
    - Consentimiento
    - Calidad
    - Proporcionalidad
    - Información
    - Responsabilidad
- **Deberes**
    - Medidas de Seguridad
    - Confidencialidad

DEBERES DEL TRATAMIENTO

SEGURIDAD

Implementar medidas de seguridad de carácter administrativo, físico y técnico que garanticen la confidencialidad, integridad y disponibilidad de los datos personales.

DEBERES DEL TRATAMIENTO

Para la adopción de una medida de seguridad u otra, el responsable deberá considerar:

I. El **valor potencial cuantitativo o cualitativo** que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión;
II. La **sensibilidad** de los datos personales tratados;
III. El **desarrollo tecnológico**;
IV. Las **posibles consecuencias de una vulneración** para los titulares;
V. Las **transferencias** de datos personales que se realicen;
VI. El **número de titulares**, y
VII. Las **vulneraciones previas ocurridas** en los sistemas de tratamiento.

Art. 17, fracción I,
LG: Ejemplos

DEBERES DEL TRATAMIENTO

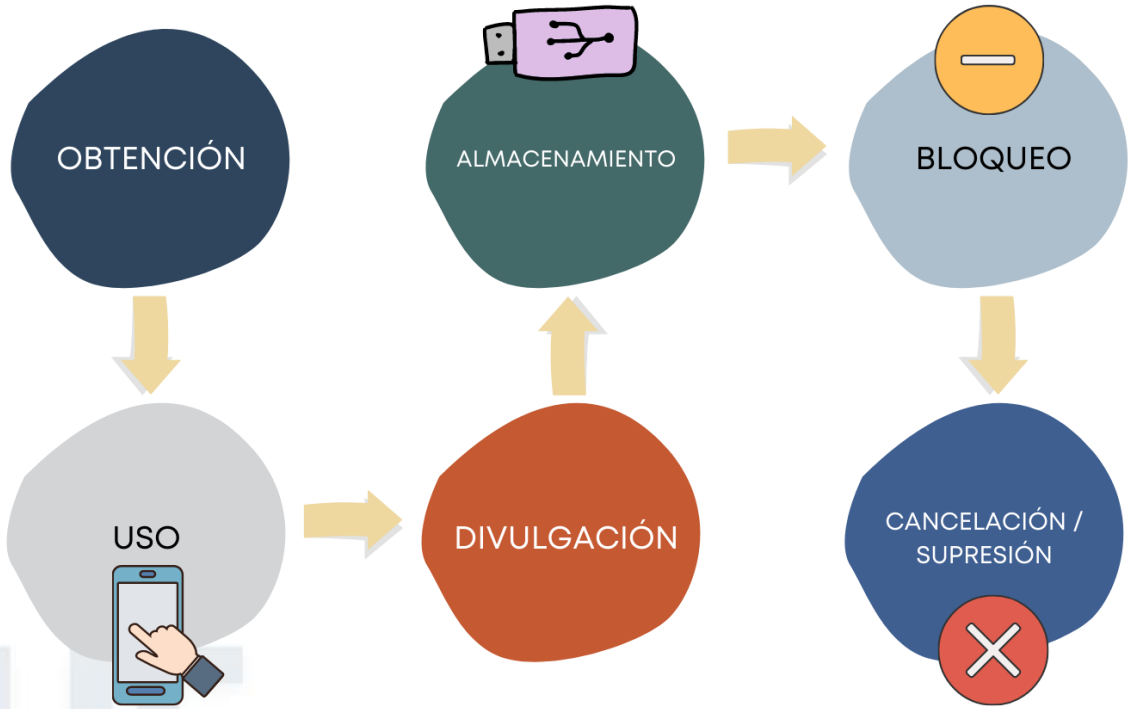
Para establecer las medidas de seguridad, el responsable deberá realizar una serie de actividades interrelacionadas:

I. Crear **políticas internas** de tratamiento de datos personales;
II. Definir las **roles, funciones y obligaciones** del personal involucrado;
III. Elaborar un **inventario** de los datos personales y de las bases de datos (e identificar el **ciclo de vida** de los datos personales);
IV. Realizar un **análisis de riesgo**, considerando las amenazas y vulnerabilidades existentes y los recursos involucrados;
V. Realizar un **análisis de brecha**;
VI. Elaborar un **plan de trabajo** para la implementación de las medidas de seguridad faltantes;
VII. Monitorear y **revisar** de manera periódica las **medidas de seguridad** implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y
VIII. Elaborar un programa de **capacitación** y capacitar al personal.

SISTEMA DE GESTIÓN

* Ciclo vital del tratamiento: cuáles son las actividades que integran cada etapa del tratamiento, desde que se obtienen hasta que se suprimen:

El ciclo de vida de los datos (en términos de la Ley):



DEBERES DEL TRATAMIENTO

- Identificar el riesgo inherente a cada tipo y categoría de dato personal

  - Nivel estándar (**verde**): datos de contacto, de identificación, académicos, laborales, etc. Son datos que simplemente pueden causar una ligera molestia en la esfera jurídica del titular.
  - Nivel sensible (**amarillo**): datos patrimoniales, ubicación física, jurídicos, etc. Son datos personales que inciden en la esfera más íntima del titular, pero sin llegar a ponerle en una potencial situación de grave peligro, discriminación o afectación a otros intereses, derechos o libertades.
  - Nivel sensible especial (**rojo**): datos de salud, datos biométricos, datos genéticos, ideología, creencias religiosas, preferencias y orientación sexual, etc. Son datos personales que inciden en la esfera más íntima del titular, y llegan a ponerle en una potencial situación de grave peligro, discriminación o afectación a otros intereses, derechos o libertades.

Tipo de dato	Nivel
Datos de identificación	Estándar
Datos de contacto	Estándar
Datos laborales	Estándar
Datos sobre procedimientos judiciales o administrativos	Sensible
Datos clínicos	Especial

DEBERES DEL TRATAMIENTO

* Realizar un análisis de riesgo, considerando las amenazas y vulnerabilidades existentes y los recursos involucrados.

¿Qué elementos deben ser identificados para la valoración del riesgo?:

- Activos (de información y de apoyo, y éstos, a su vez, físicos o electrónicos / digitales)
- Vulnerabilidades
- Amenazas
- Daño
- Probabilidad

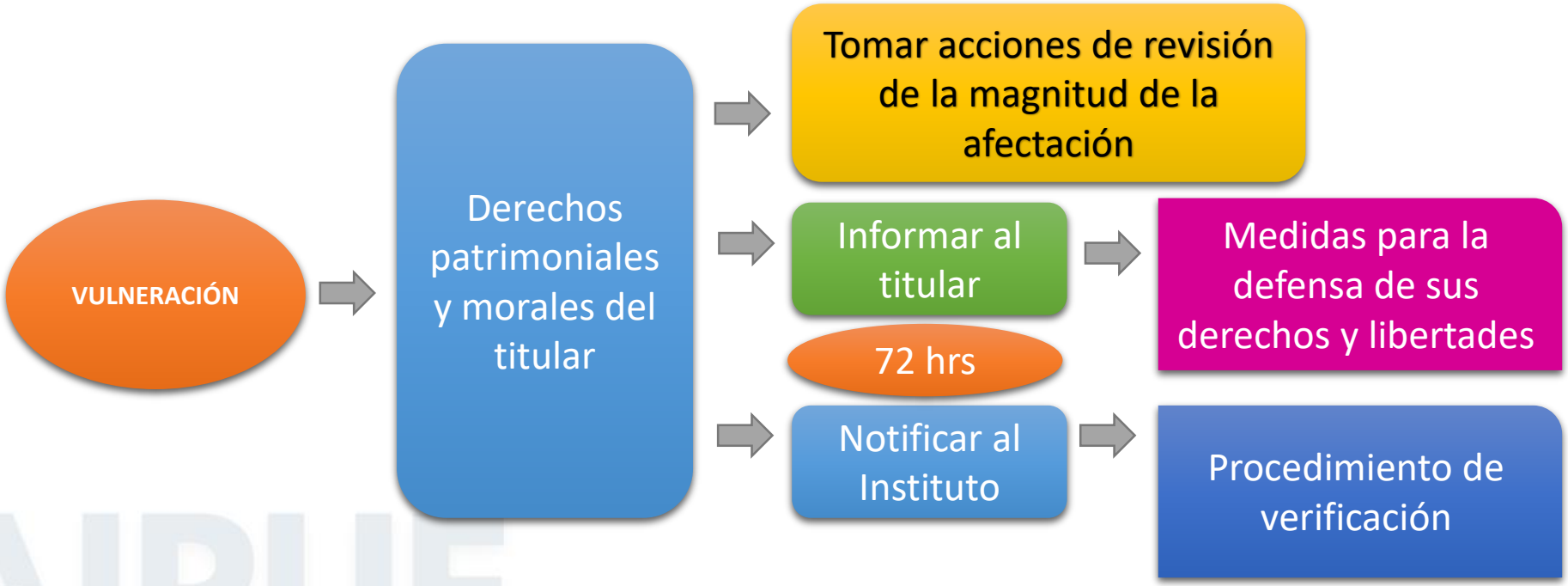
DEBERES DEL TRATAMIENTO

El responsable deberá elaborar, además, un **documento de seguridad** que contenga, al menos, lo siguiente:

I. El **inventario** de datos personales y de los sistemas de tratamiento;
II. Las **funciones y obligaciones** de las personas que traten datos personales;
III. El **análisis de riesgos**;
IV. El **análisis de brecha**;
V. El **plan de trabajo**;
VI. Los **mecanismos de monitoreo y revisión** de las medidas de seguridad;
VII. El **programa general de capacitación**, y
VIII. **Nombre y cargo del personal** del responsable o encargado.

El responsable deberá llevar una **bitácora de vulneraciones a la seguridad** ocurridas y en la que se describa:

I. La fecha en la que ocurrió;
II. El motivo de la vulneración de seguridad, y
III. Las acciones correctivas implementadas de forma inmediata y definitiva.



DEBERES DEL TRATAMIENTO

CONFIDENCIALIDAD

El responsable deberá establecer controles o mecanismos que tengan por objeto que el personal involucrado en el tratamiento de datos personales guarde confidencialidad respecto de éstos.

Esta obligación subsistirá incluso después de finalizar la relación con el responsable.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
DOF: 26/01/2017
http://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del **Estado de Puebla**
POEP: 26/07/2017
http://www.itaipue.org.mx/documentos/Ley_de_Proteccion_de_Datos_Personales_en_Posesion_de_SujetosObligados_estatal.pdf

Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla
POEP: 19/06/2018
http://www.itaipue.org.mx/documentos/LineamientosGeneralesPDP-PSO-EdoPuebla.pdf

Lineamientos que establecen los parámetros, modalidades y procedimientos para la **portabilidad** de datos personales
DOF: 12/02/2018
http://www.itaipue.org.mx/documentos/Lineamientos_portabilidad.pdf

Disposiciones administrativas de carácter general para la elaboración, prestación y valoración de **evaluaciones de impacto** en la protección de datos personales
DOF: 23/01/2018
http://www.itaipue.org.mx/documentos/Lineamientos_evaluaciones_de_impacto.pdf

Criterios generales para la instrumentación de **medidas compensatorias** en el sector público del orden federal, estatal y municipal
DOF: 23/01/2018
http://www.itaipue.org.mx/documentos/Criterios_generales_medidas_compensatorias.pdf

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE PUEBLA

Manuel Ángel Díaz Martínez.
Subdirección de Datos Personales
manuel.diaz@itaipue.org.mx