INSTITUTO DE Transparencia BAJA CALIFORNIA

Deberes para la protección de los datos personales y Sistema de Gestión

Última actualización: 23 de agosto, 2023.

-Deberes para la protección de datos personales

Contenido:

-Marco jurídico

-¿En qué consiste el deber de Confidencialidad?

-¿En qué consiste el deber de Seguridad?

-Medidas de seguridad administrativas

-Medidas de seguridad físicas

-Medidas de seguridad técnicas

-Conceptos

-Cumplimiento de deberes

Marco jurídico

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Artículos 31 al 42

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California
Artículos 16 al 21

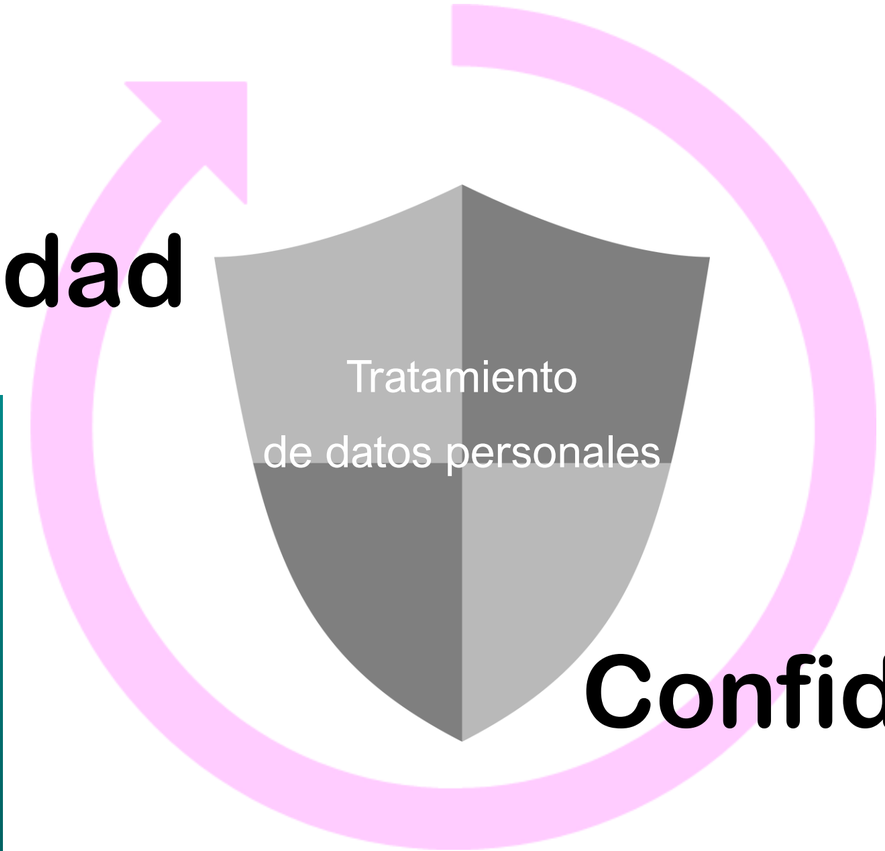
Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California
Artículos 57 al 84

La documentación generada por el SO responsable:
Lineamientos, programas, políticas. contratos, convenios, consentimientos, avisos de privacidad, etc.

Deberes para la protección de datos personales

Seguridad

El responsable debe establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para proteger los datos personales



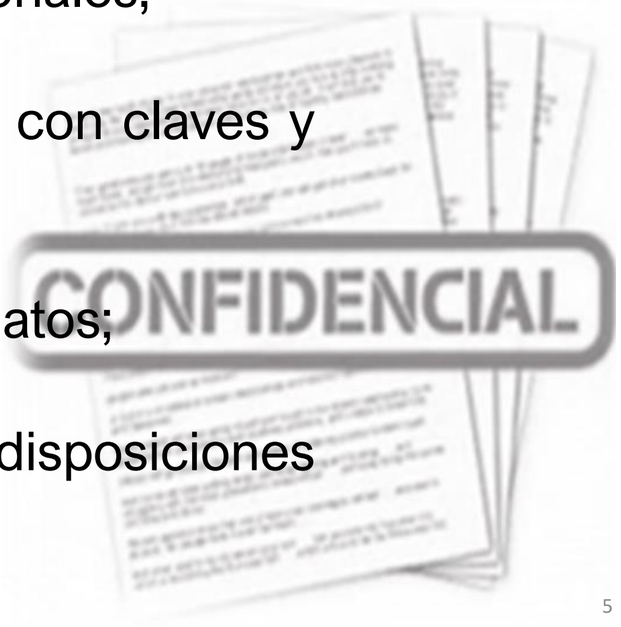
Confidencialidad

El responsable debe establecer controles o mecanismos a efecto de que todas las personas que intervienen en cualquier fase del tratamiento de datos personales, guarden confidencialidad con relación a estos, obligación que subsiste aun después de finalizar sus relaciones con el mismo.

Actividades para cumplir con el deber de confidencialidad

- ❑ Capacitar a las personas servidoras públicas sobre el uso correcto de los activos y de las bases de datos;
- ❑ **Suscribir cláusulas de confidencialidad con quienes intervengan en los tratamientos de datos personales**;
- ❑ Imposición de sanciones por la revelación no autorizada de datos personales;
- ❑ Que el personal autorizado para ingresar a las bases de datos cuente con claves y contraseñas de acceso;
- ❑ Establecer manuales de procedimientos sobre el uso de las bases de datos;

Las que el sujeto obligado determine, siempre que no contravengan las disposiciones en la materia



Medidas de seguridad administrativas

Implementación de **políticas y procedimientos** para la gestión, soporte y revisión de la seguridad de la información **a nivel organizacional;** la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

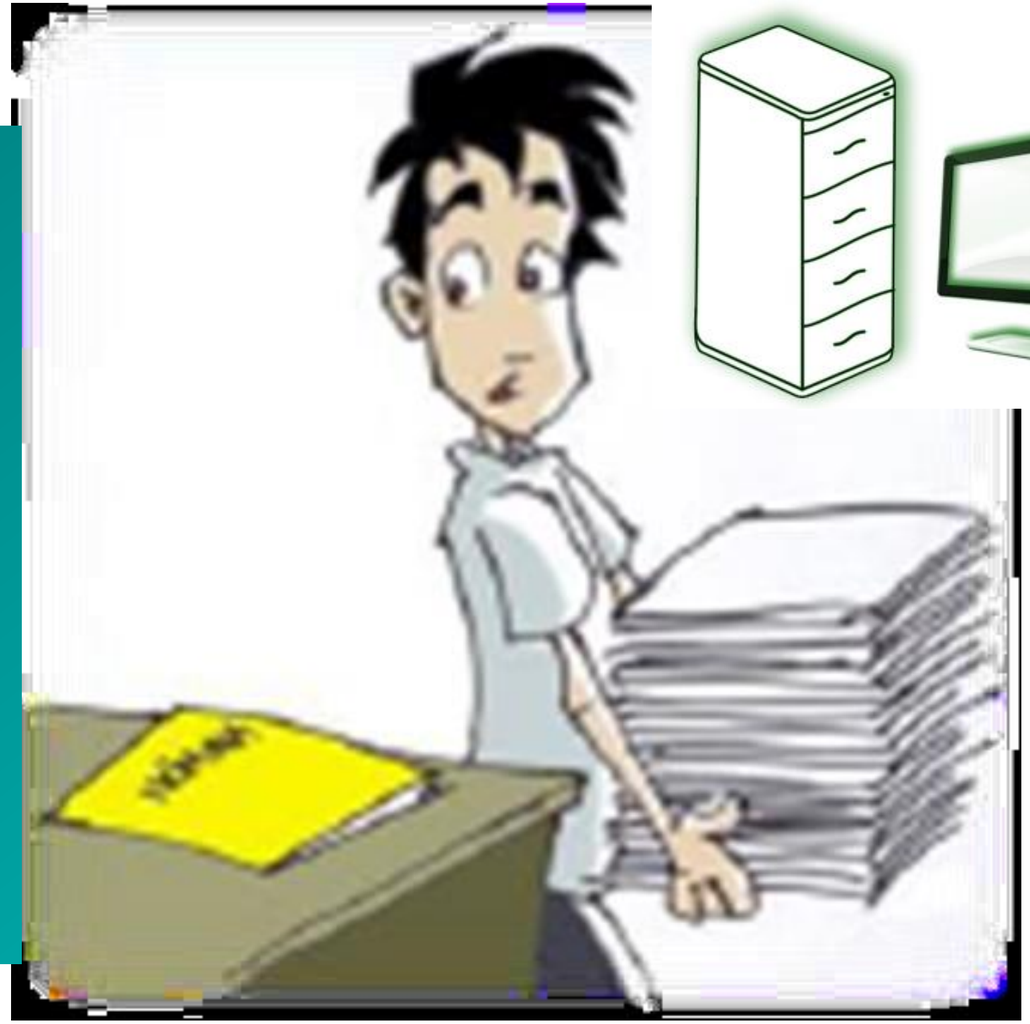
Medidas de seguridad administrativas

- **Políticas de protección de datos personales**;
- **Identificar roles y perfiles de quienes tratan datos personales**;
- Asignación de derechos de los usuarios para el acceso a las bases de datos;
- Implementar protocolos de seguridad;
- **Avisos de privacidad**;
- Formatos para la obtención del consentimiento;
- Cláusulas de confidencialidad;
- Contratos con encargados;
- **Programa de capacitación interno en materia de protección de datos personales;**
- Documentar procedimientos y periodos de conservación de las bases de datos, así como para el bloqueo y supresión de los datos;
- Emitir reglamentación interna que contemple sanciones;
- Elaborar el inventario de tratamientos de datos personales;
- **Elaborar el documento de seguridad**.

Medidas de seguridad físicas

Conjunto de **acciones y mecanismos** para **proteger el entorno físico** de los datos personales y de los activos involucrados en su tratamiento.

activos: instalaciones, archiveros, oficinas, equipos de cómputo, cajones, almacén (archivo)



Medidas de seguridad físicas

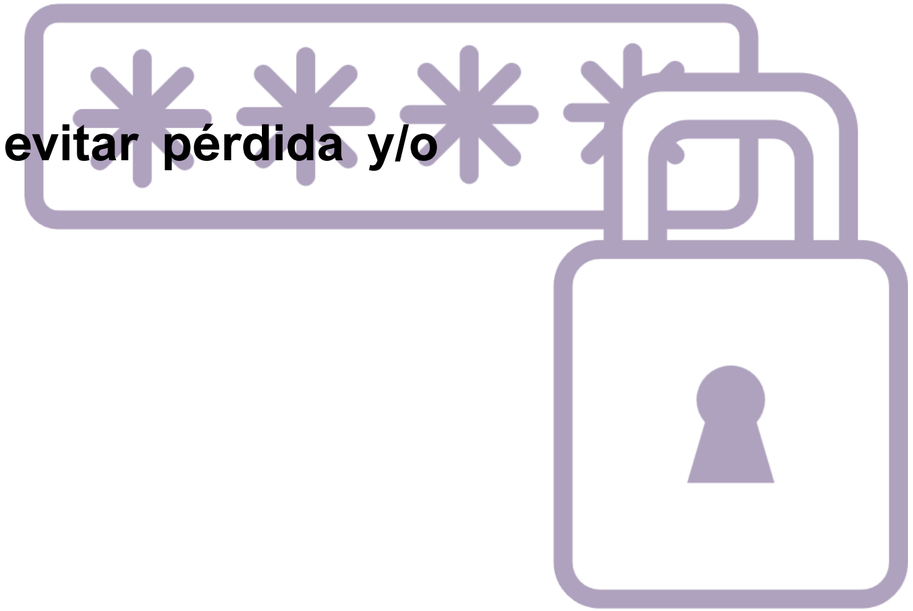
- Prevenir el acceso no autorizado a las instalaciones físicas, áreas críticas, recursos e información;
- Colocar señalamientos visuales en áreas de acceso restringido (solo personal autorizado);
- Instalar cámaras de seguridad, vigilancia;
- Proveer infraestructura que proteja los datos de humedad, polvo, temperatura o plagas;
- Utilizar candados, cerraduras y/o tarjetas de identificación para que solo las personas autorizadas puedan acceder a las bases de datos;
- Establecer un sistema de vigilancia, alarmas y prevención contra siniestros;
- Proveer mantenimiento a los equipos que contienen o almacenan datos personales;

Medidas de seguridad técnicas

Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para **proteger el entorno digital** de los datos personales y los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas

- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware;
- Realizar copias se seguridad y respaldos de los datos; Encriptación y cifrado;
- Proteger los recursos móviles y portátiles con el uso de sensores;
- Deshabilitar y/o cancelar puertos de comunicación (usb) y dispositivos de almacenamiento removible;
- **Instalación de firewalls, antivirus y mecanismos para evitar pérdida y/o filtración de datos**;
- Instalar reguladores de voltaje en los equipos de cómputo.



Conceptos

Tratamiento

Operaciones manuales o automatizadas aplicadas a los datos personales, desde su obtención hasta su disposición final.

Conceptos

Base de datos

Conjunto de datos referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia del tipo de soporte u organización.

Conceptos

Sistema de tratamiento

Conjunto de bases de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Conceptos

Activos

Todo elemento involucrado en el tratamiento de datos personales, y que por lo tanto tienen un valor para la organización.

- Activos de Información
- Activos de Apoyo

Conceptos

Amenaza

Circunstancia o condición externa, con lo capacidad de causar daño a los activos.

Conceptos

Vulnerabilidad

Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

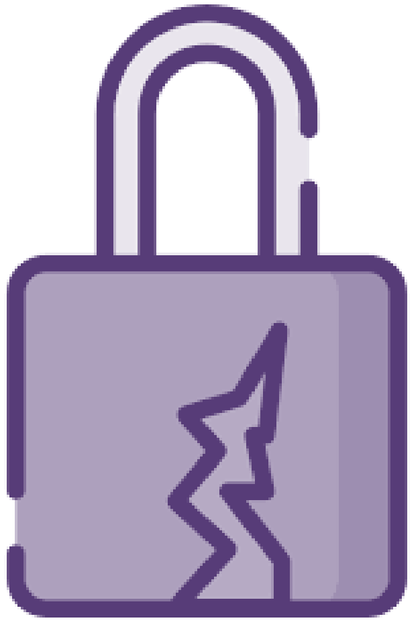
Conceptos

Riesgo

Probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes en un activo o grupo de activos, y que éste cause un impacto negativo o daño

Conceptos

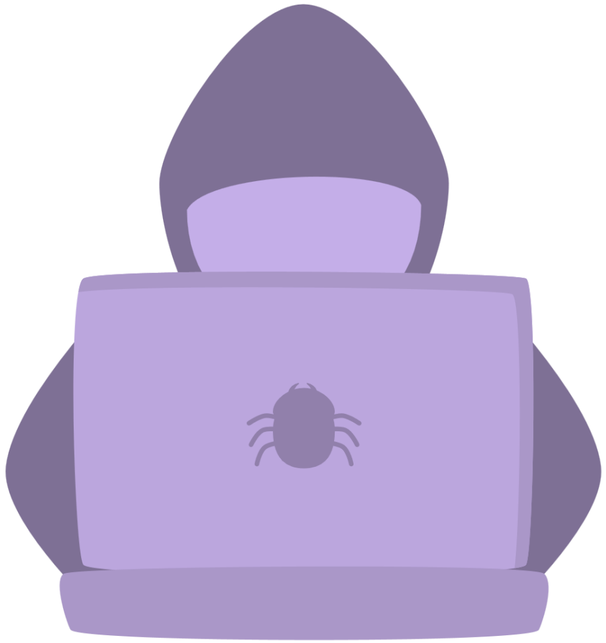
Incidente de seguridad



Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información.

Conceptos

Vulneración de seguridad



Incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento.

Conceptos

Medidas de seguridad

Acciones o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.

-Sistema de Gestión de Seguridad de Datos Personales

Contenido:

-¿Qué es un Sistema de Gestión?

-Funciones de la persona oficial de protección de datos

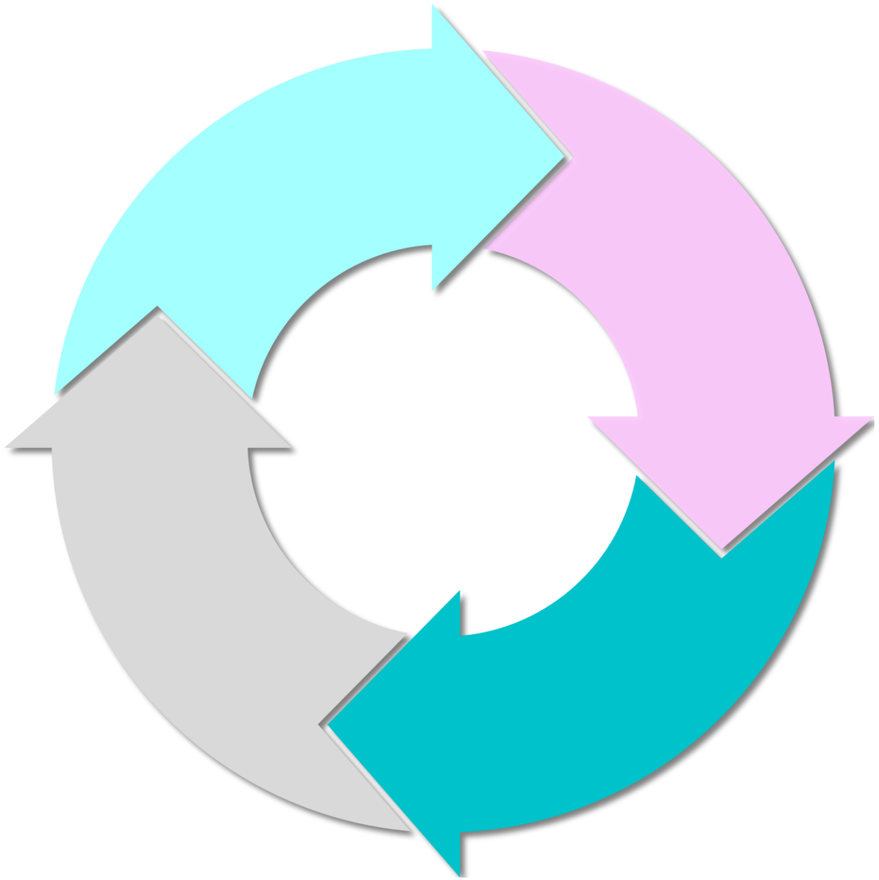
-Elementos del Sistema de gestión

-Fases del Sistema de Gestión:

- -1. Planear.
- -2. Implementar.
- -3. Monitorear.
- -4. Mejorar.

-Documento de Seguridad

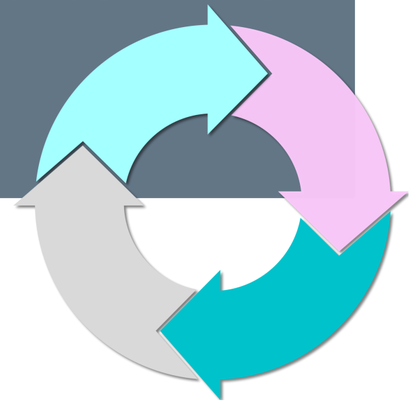
¿Qué es un Sistema de Gestión?



Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Funciones de la persona oficial de protección de datos

La persona oficial de protección de datos tiene a su cargo la responsabilidad de coordinar la implementación de un programa integral de PDP en la organización del SO. →**SG**



Elementos del sistema de gestión

I. Políticas de gestión y tratamiento de datos personales

II. Funciones y obligaciones del personal que trata datos personales

III. Inventario de datos personales y sistemas de tratamiento

IV. Análisis de riesgos de los sistemas de tratamiento

V. Análisis de brecha de las medidas de seguridad

VI. Plan de trabajo sobre medidas de seguridad

VII. Monitoreo y revisión periódica de las medidas de seguridad

VIII. Capacitación basada en niveles

El **deber de seguridad** se materializa mediante la implementación de un

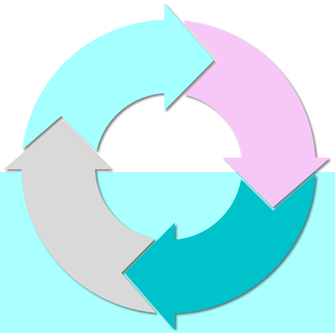
Sistema de Gestión de Seguridad de Datos Personales

Para ello, el INAI recomienda el "Programa de Protección de Datos".

Documento Orientador.

Versión agosto de 2018

Elementos del Programa de Protección de Datos Personales



Paso 1.	Establecer el Alcance y los Objetivos	I.
Paso 2.	Elaborar una Política de Gestión de Datos Personales	II.
Paso 3.	Establecer Funciones y Obligaciones	III.
Paso 4.	Elaborar el Inventario de Datos Personales	IV.
Paso 5.	Realizar un Análisis de Riesgo de datos personales	V.
Paso 6.	Realizar un Análisis de Brecha de las medidas de seguridad	
Paso 7.	Implementar las medidas de seguridad aplicables a los datos personales → Plan de trabajo	VI.
Paso 8.	Revisiones y Auditoría	VII.
Paso 9.	Mejora continua y Capacitación	VIII.

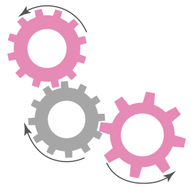
El documento orientador advierte...

AVISO

...se trata de una referencia y un esquema con la descripción del marco general de medidas y acciones que se consideran necesarias implementar con relación a las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el sector Público.

Esta información no es vinculante para los sujetos obligados, sino que constituye una de las herramientas de facilitación y orientación que elabora la Dirección General de Prevención y Autorregulación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para apoyar a los sujetos obligados en el cumplimiento de sus obligaciones en materia de protección de datos personales.

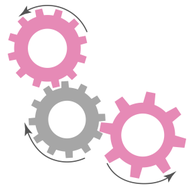
Al ser un ejemplo, resulta indispensable que, para el buen funcionamiento e implementación del Programa de Protección de Datos Personales, los sujetos obligados realicen las actualizaciones, adaptaciones y precisiones necesarias según las características propias de su institución.



Así, la implementación del Programa requiere de las siguientes acciones generales, además de las específicas que tendrá que realizar cada unidad administrativa para cumplir con sus obligaciones en materia de protección de datos personales:

- 1. Elaboración del inventario de tratamientos, que permitirá tener un diagnóstico y mapeo de los tratamientos que realiza la organización y que es necesario para poder cumplir con el resto de las obligaciones.
- 2. Elaboración del análisis de riesgo y el de brecha, así como el programa respectivo para la implementación de las medidas de seguridad.
- 3. Actualización o elaboración del Documento de Seguridad de la organización.
- 4. Elaboración de procedimientos internos para la atención de solicitudes de derechos de acceso, rectificación, cancelación y oposición, y lo relativo a la portabilidad;
- 5. Elaboración o actualización del programa de capacitación para los servidores públicos en materia de protección de datos personales.
- 6. Elaboración de un programa de revisiones y auditorías sobre la implementación del Programa.
- 7. Desarrollo de procedimientos y mecanismos para:

o La conservación y supresión de datos personales;
o La identificación de vulneraciones y su respectiva notificación;
o El bloqueo de los datos personales;
o La presentación de las Evaluaciones de Impacto a la Protección de Datos Personales, y
o La supervisión de la aplicación del Documento de Seguridad.



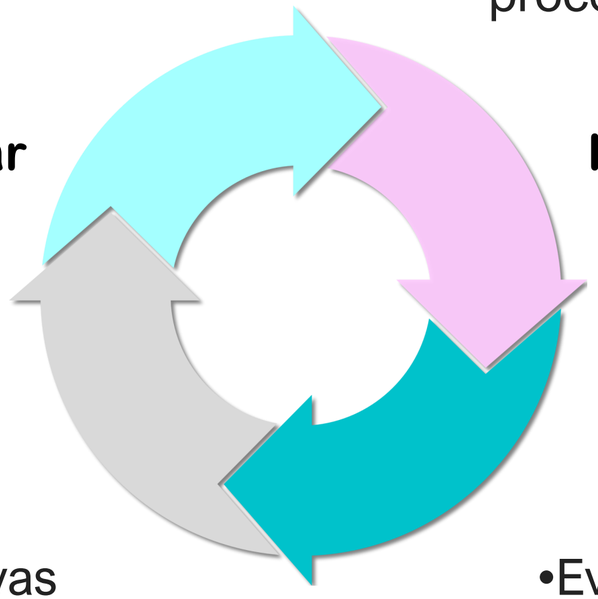
Sitema de Gestión
Fases

I. Planear

•Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos

II. Implementar

•Implementar y operar las políticas, objetivos, planes, procesos y procedimientos



III. Monitorear

•Evaluar los resultados de lo implementado; verificar el adecuado funcionamiento del sistema de gestión

IV. Mejorar

•Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión realizada, para lograr la mejora continua

Fase 1. Planear.

Paso 1. Establecer el alcance y objetivos

¿Hasta dónde queremos llegar?

Aplicable a todas las unidades administrativas y personas servidoras públicas que realicen tratamientos de datos personales en ejercicio de sus atribuciones, así como a los encargados, en su caso.

¿Qué queremos lograr?

Cumplir con las obligaciones establecidas en la LPDPPSOBC y sus Lineamientos, atendiendo a los principios, deberes y derechos rectores de la protección de datos personales.

Fase 1. Planear

Paso 2. Elaborar una política de gestión de datos personales

ESTRUCTURA DE UNA POLÍTICA					
¿Qué?		¿Quién?	¿Por qué?	¿Cómo?	¿Cuándo/donde?
¿Qué voy a proteger?		¿Quién lo va a proteger?	¿Cuál es la razón y la acción?		¿Cuál es el periodo?
Activo(s) de Información	Activo(s) de Apoyo	Responsable/Encargado/ Custodio	Razón del Tratamiento	Acción	Periodo de conservación
Información que genera la organización -Datos personales -Procesos -Actividades involucradas en el tratamiento de datos personales	Activos en los que reside la información -Hardware -Software -Redes y Telecomunicaciones -Personal -Estructura	Establecer una cadena de rendición de cuentas	Establecer finalidades	Tomar en cuenta el ciclo de vida de los datos personales	

Fase 1. Planeación

Paso 3. Establecer funciones y obligaciones

Funciones y obligaciones de los que tratan datos personales

Identificar al **personal** que realiza tratamiento de datos personales

Saber que **tipo de tratamiento** realiza con base al ciclo de vida de los DP

Conocer los **riesgos** asociados al tratamiento que realiza

Definir **medidas de seguridad** para atender los riesgos identificados

- Establecer **perfiles y privilegios** adecuados
- Definir **responsabilidades** para la protección de los DP
- Establecer **cadena de rendición de cuentas**, en caso de vulneraciones de seguridad
- Identificar requerimientos específicos en materia de **capacitación** de DP

Cadena de rendición de cuentas.

Comité de transparencia

Autoridad máxima en materia de protección de datos personales

Autoridad máxima dentro de la organización (titular del SO)

Apoyo de la más alta jerarquía para impulsar el programa

Oficial de Protección de datos

Coordinar el cumplimiento de obligaciones de pdp

Unidad de transparencia

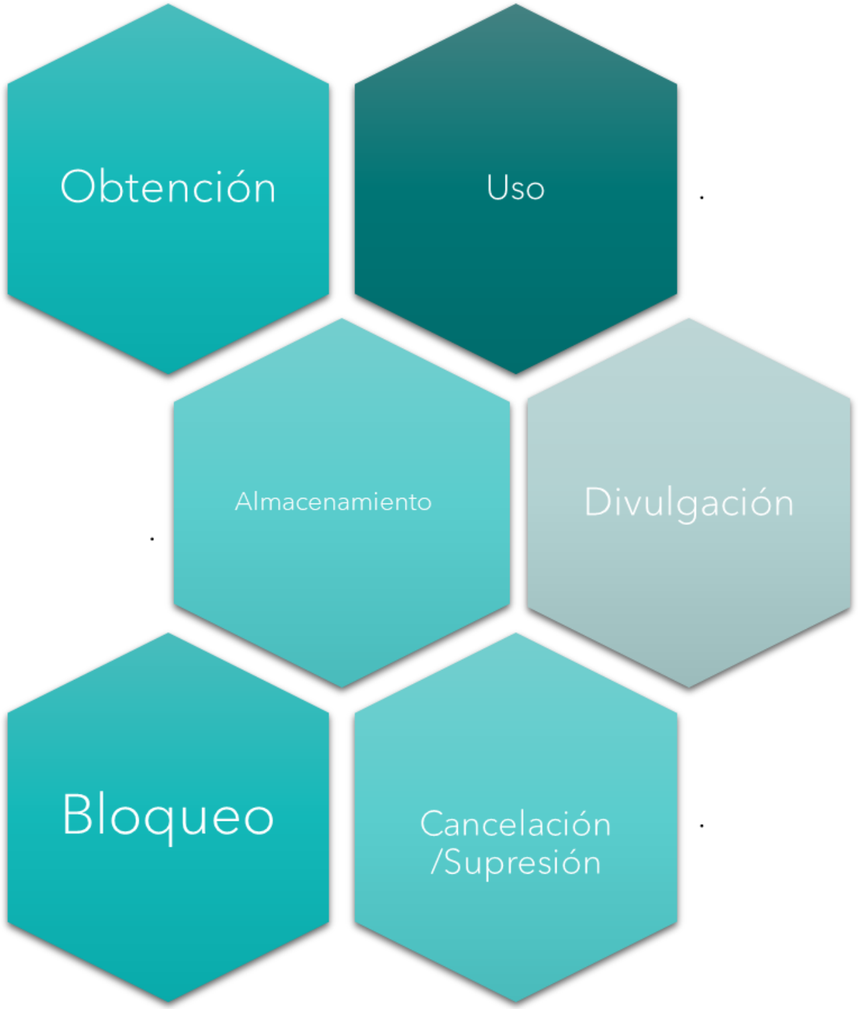
Gestiona las solicitudes de protección de datos personales ARCOP

Unidades Administrativas

Aplican medidas de seguridad a sus bases de datos y sistemas de tratamiento y llevan a la práctica los principios y deberes de pdp

Fase 1. Planeación

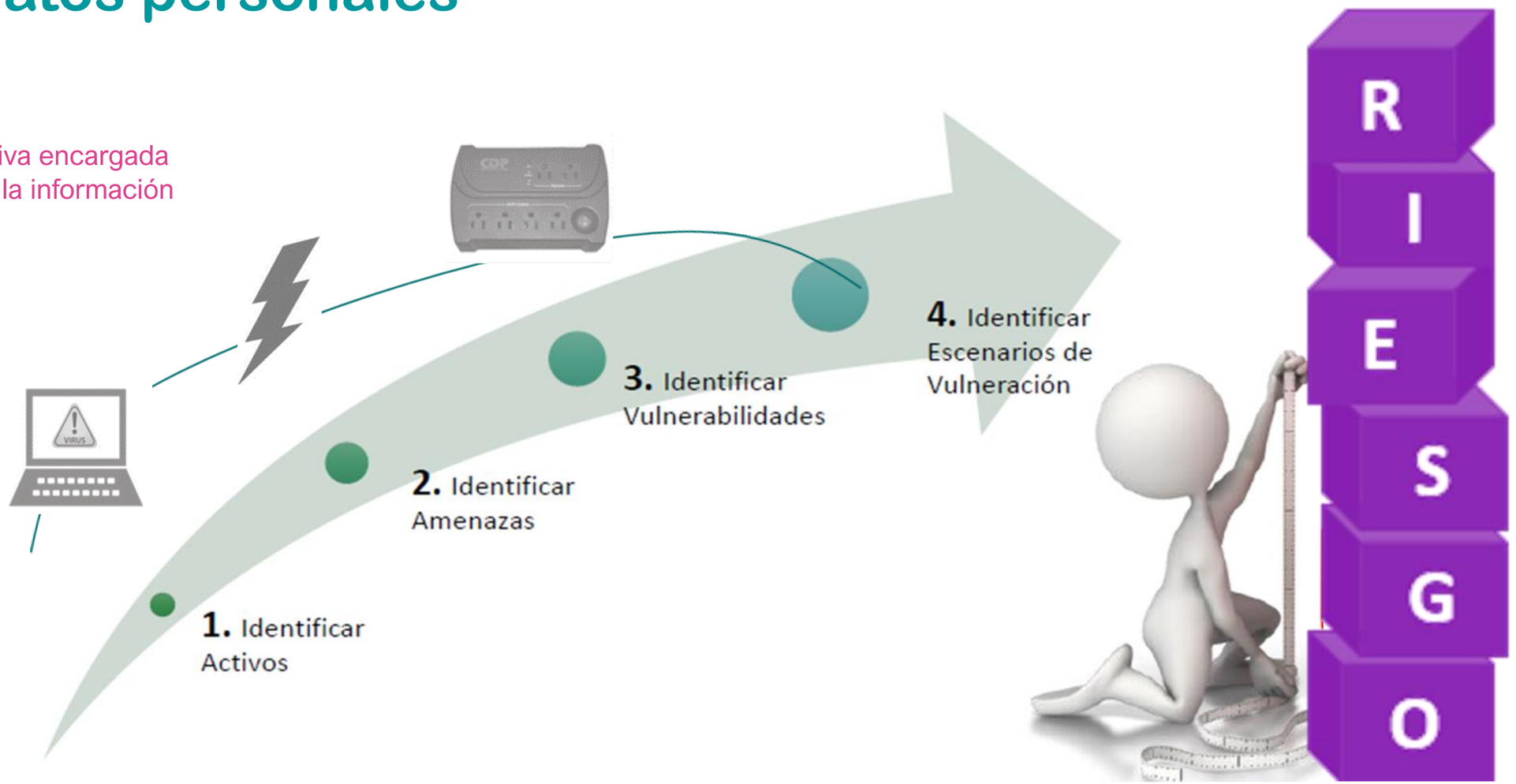
Paso 4. Elaborar el inventario de sistemas de datos personales



Fase 1. Planeación

Paso 5. Realizar un análisis de riesgos de los datos personales

Unidad administrativa encargada de la seguridad de la información



Bitácora de riesgos

					análisis de brecha
EQUIPOS DE CÓMPUTO	VIRUS	EQUIPOS SIN ANTIVIRUS	BORRADO PERMANENTE DE INFORMACIÓN	MUY PROBABLE	?
ACTIVO	**AMENAZA**	**VULNERABILIDAD**	**DAÑO / IMPACTO**	**POTENCIAL / PROBABILIDAD**	**MEDIDA DE SEGURIDAD**
EXPEDIENTES FÍSICOS	INCENDIO	MATERIAL SUSCEPTIBLE AL FUEGO	PÉRDIDA DEFINITIVA DE LA INFORMACIÓN	POCO PROBABLE	?

Fase 1. Planeación

Paso 6. Realizar un análisis de brecha de las medidas de seguridad

Unidad administrativa encargada de la seguridad de la información

Identificar:

- Las medidas de seguridad existentes;
- Las medidas de seguridad existentes que operan correctamente;
- Las medidas de seguridad faltantes;
- Si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados actualmente.

Fase 2. Implementación

Paso 7. Implementar las medidas de seguridad aplicables a los datos personales

Unidad administrativa encargada de la seguridad de la información

Plan de trabajo

- Debe reflejar los recursos disponibles: humanos, económicos, de conocimiento y de tiempo con los que se cuenta.

Debe contener al menos:

- Las acciones prioritarias;
- El periodo en el que se pretende cumplir las acciones;
- Las personas encargadas de cumplir con las acciones.

Fase 3. Monitoreo

Paso 8. Revisiones y auditoria

Programa de auditoria

- Monitorear continuamente:
  - Los activos de la gestión de riesgos;
  - Las modificaciones realizadas a los activos;
  - Las amenazas existentes;
  - Las vulnerabilidades de los activos;
  - El impacto de amenazas, vulnerabilidades y riesgos en conjunto;
  - Los incidentes y vulneraciones ocurridas con anterioridad.

Evaluar y medir los resultados de las políticas, planes, procesos y procedimientos

Medir la eficacia y eficiencia del SGSDP

Paso 9. Mejora continua y capacitación

Programa de capacitación

- Dirigido al personal;
- Dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Documento de Seguridad

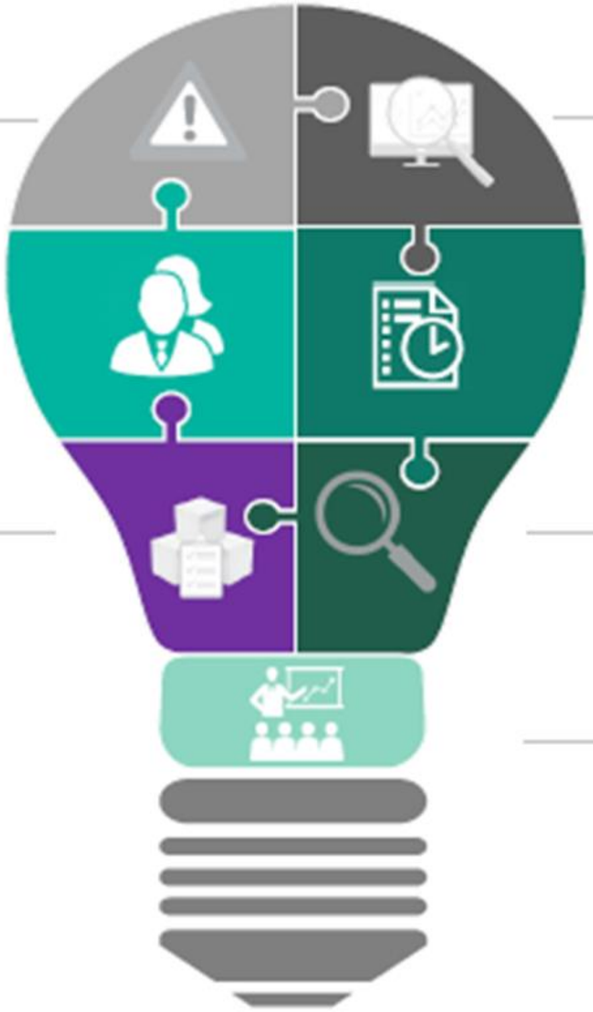
Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Contenido del Documento de Seguridad

III. Análisis de riesgos

II. Funciones y obligaciones

I. Inventario de datos personales



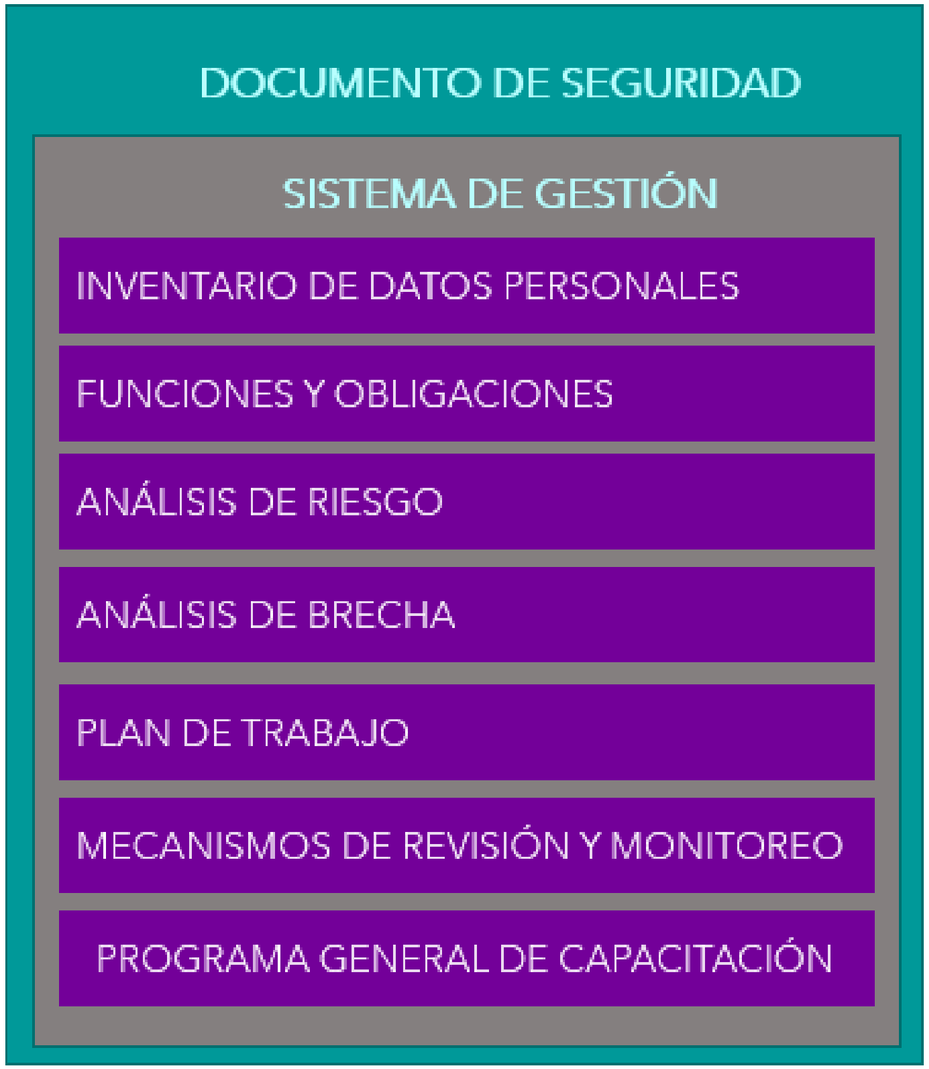
IV. Análisis de brecha

V. Plan de trabajo

VI. Mecanismos para monitoreo y revision medidas de seguridad

VII. Programa general de capacitación

¿Cuándo se actualiza el Documento de Seguridad?



- Cuando se produzcan modificaciones sustanciales al tratamiento de datos personales, que impliquen un cambio en el nivel de riesgo;
- Atendiendo a una mejora continua, por el monitoreo y revisión del sistema de gestión;
- Como parte de las acciones de un proceso de mejora, para disminuir el impacto de una vulneración a la seguridad;

Denuncia PDP

Lineamientos de protección de datos personales en posesión de sujetos obligados del Estado de Baja California

Artículo 84

La carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en el presente Capítulo recaerá, en todo momento, en el responsable.

Artículo 199

Las investigaciones previas podrán iniciar:

II. A petición de parte: por denuncia del titular cuando considere que ha sido afectado por actos del responsable, o por cualquier persona cuando se tenga conocimiento de presuntos incumplimientos a las obligaciones de la Ley.

Herramientas de apoyo

ITAIPBC

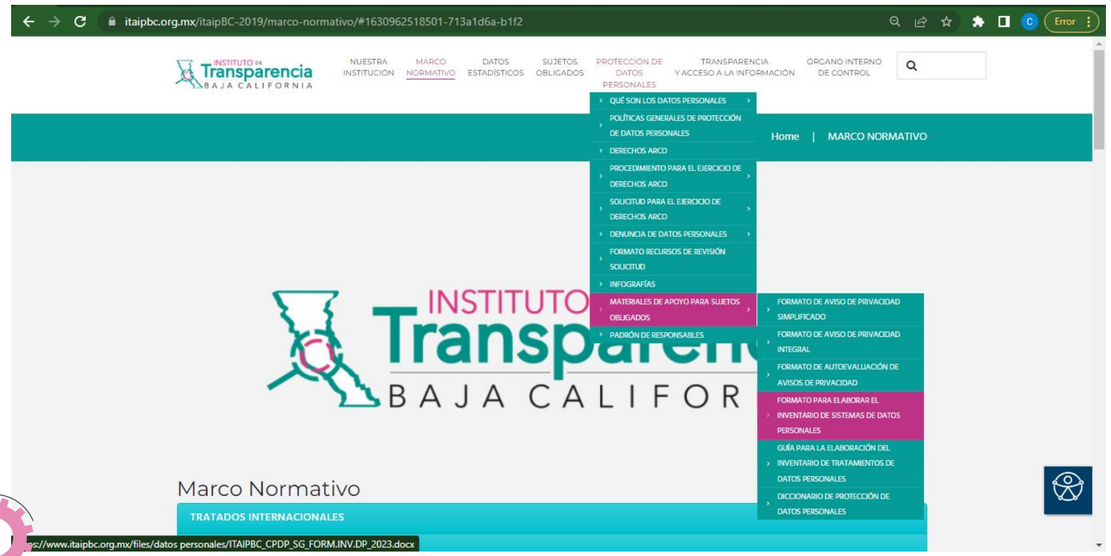
http://www.itaipbc.org.mx/itaipBC-2019/
MENÚ: PROTECCIÓN DE DATOS PERSONALES

→Formato para la elaboración del inventario de sistemas de datos personales

→Guía para la elaboración del inventario de sistemas de datos personales

→Formato para la elaboración del aviso de privacidad simplificado

→Formato para la elaboración del aviso de privacidad integral



INAI

https://home.inai.org.mx/
MENÚ: PROTECCIÓN DE DATOS PERSONALES

→Programa de Protección de Datos. Documento Orientador. Versión agosto de 2018
https://home.inai.org.mx/?page_id=3420

→ Recomendaciones para la elaboración de políticas internas de gestión y tratamiento de datos personales
https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/RecomendacionesPol%C3%ADticasPDP.pdf

→Recomendaciones para el manejo de incidentes de seguridad de Datos Personales
https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones_Manejo_IS_DP.pdf

→Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo
https://home.inai.org.mx/wp-content/uploads/AmenazasDP.pdf

Guía para la elaboración del Documento de Seguridad
https://home.inai.org.mx//wp-content/documentos/DocumentosSectorPublico/Guia-apoyo-DS.pdf

INSTITUTO DE Transparencia BAJA CALIFORNIA

CPDP Coordinación de Protección de Datos Personales

Mariela Juárez L.

(664) 621 1305

datospersonales@itaipbc.org.mx

http://www.itaipbc.org.mx/itaipBC-2019