idaip Quintana Roo
Por tu derecho a saber

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Protección de Datos Personales: Documento de Seguridad

27 de enero de 2022

Dra. Gabriela Inés Montes Márquez

Legislación en materia de datos personales en posesión de sujetos obligados

Constitución Política de los Estados Unidos Mexicanos

Ámbito Federal

Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

Ámbito local

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo

Principios y deberes

Reconoce 4 derechos a los particulares

1. Acceso
2. Rectificación
3. Cancelación
4. Oposición

* Además se reconoce el derecho a la Portabilidad de datos

Establece obligaciones a los sujetos obligados

8 principios

1. Licitud
2. Lealtad
3. Consentimiento
4. Finalidad
5. Proporcionalidad
6. Información
7. Calidad
8. Responsabilidad

2 deberes

1. Seguridad
2. Confidencialidad

Deber de Seguridad

Consiste en garantizar que únicamente el responsables de los datos podrá llevar a cabo el tratamiento de los mismos, por lo que deberá adoptar medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, las cuales deben sr plasmadas en el **documento de seguridad**:

- **El responsable debe:**

Establecer y mantener las medidas de seguridad administrativas, físicas y técnicas.

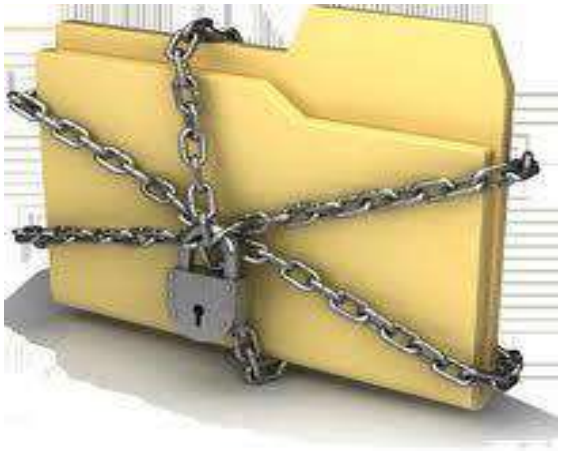
Realizar una serie de actividades interrelacionadas

Documentar las actividades mediante un **sistema de gestión.**

DOCUMENTO DE SEGURIDAD

Documento de seguridad
(Art. 3, f. XIII LPDPPSOEY)

Es el 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 que posee.



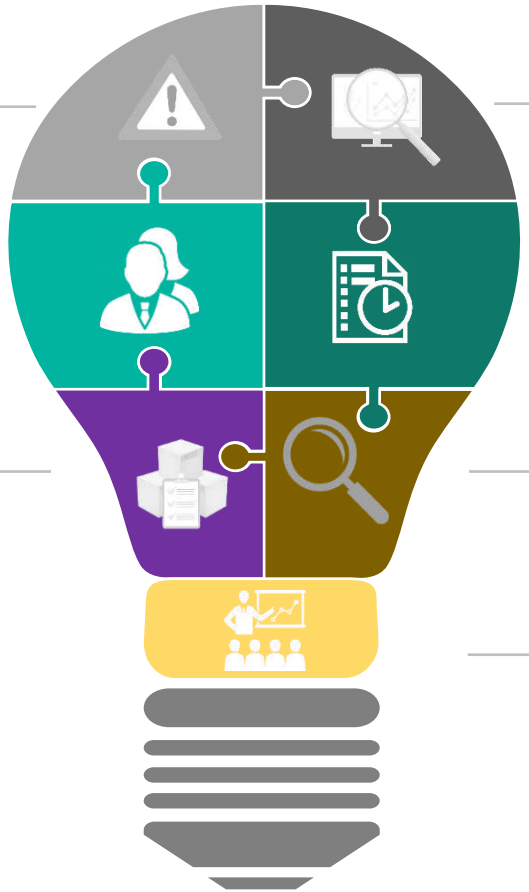
MARCO NORMATIVO

Documento de seguridad

Análisis de riesgos

Funciones y obligaciones

Inventario de datos personales



Análisis de brecha

Plan de trabajo

Mecanismos para monitoreo y revision medidas de seguridad

Programa general de capacitación

DS

Artículo 4, fr XV de la LPDPPSOQR

Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

Medidas de seguridad

El responsable deberá establecer y mantener las medidas de seguridad

- ⇨ Administrativas
- ⇨ Físicas
- ⇨ Técnicas

EVITAR

- ✘ Daño
- ✘ Pérdida,
- ✘ Alteración,
- ✘ Destrucción o
- ✘ Uso, acceso o tratamiento no autorizado,

GARANTIZAR

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Disponibilidad

Medidas de seguridad administrativas

- Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional
- Identificación, clasificación y borrado seguro de la información;
- Sensibilización y capacitación del personal, en materia de protección de datos personales;

Mantener seguros los documentos

- ✓ Evita dejar documentos a la mano.
- ✓ Resguarda tus contraseñas en un lugar seguro.
- ✓ Usar archiveros con llave.

Destruir los documentos cuando hayan dejado de ser necesarios

Evita tirar documentos con datos personales sin triturar.

No dejar documentos en la fotocopiadora.

Cuidar el reúso de papel con datos personales.

No dejar a la vista datos personales

Medidas de seguridad físicas

Conjunto de acciones y mecanismos para proteger e**l entorno físico de los datos personales y de los recursos involucrados en su tratamiento.**

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

Medidas de seguridad físicas

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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.

a) Prevenir que el acceso a las bases de datos personales o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

Medidas de seguridad técnicas

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Las medidas deben considerar

Artículo 33. …

I. El riesgo inherente a los datos personales tratados;

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;

VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y

VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Debe existir un sistema de gestión

Artículo 36. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

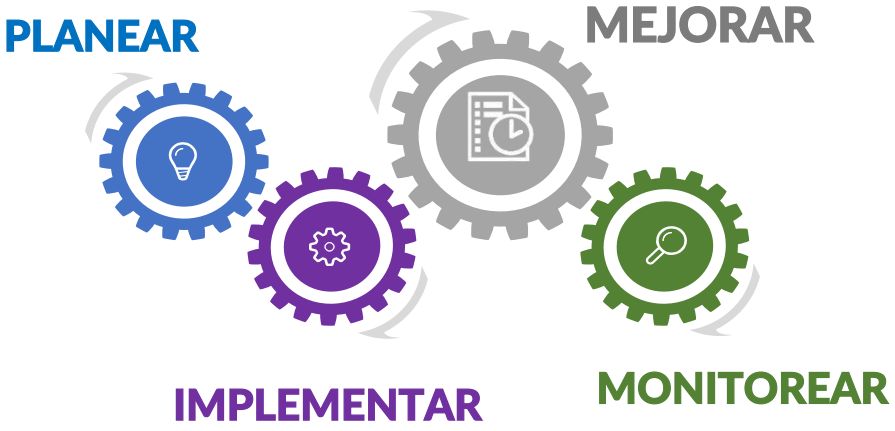
Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

Información **exacta y completa**, para ser revelada, accesible y utilizable sólo para las **personas autorizadas**.

Información correcta → para la persona correcta → en el momento correcto

Para la seguridad de los datos personales, **el INAI RECOMIENDA** la adopción de un **Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).**

bit.ly/RecomendacionesSeguridadINAI2013



MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

Políticas gestión y tratamiento de datos personales

Funciones y obligaciones del personal que trata datos personales

Inventario datos personales y sistemas de tratamiento

Análisis de riesgos para datos personales

Análisis de brecha medidas de seguridad

Plan de trabajo medidas de seguridad

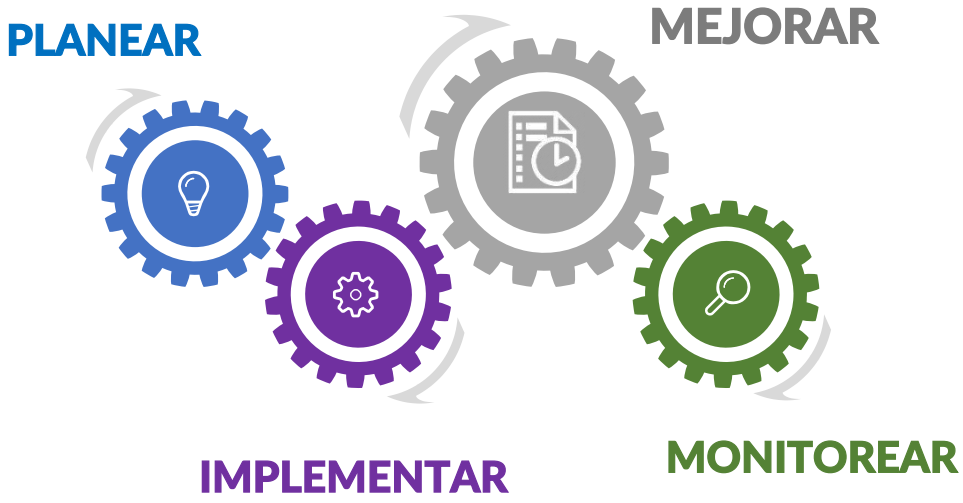
Monitoreo y revisión periódica medidas seguridad

Capacitación basada en niveles

Artículo 34 de la LGPDPPSO
Artículo 36 de la LPDPPSOEQR

Las acciones relacionadas con las **medidas de seguridad** para el tratamiento de los datos personales deberán estar documentadas y contenidas en un **sistema de gestión**.

Sistema de Gestión



Sistema de Gestión de Seguridad de Datos Personales

Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** **Elaborar un Inventario de Datos Personales** • **Paso 5.** Realizar un Análisis de Riesgo de Datos Personales • **Paso 6.** Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	• **Paso 7.** Implementación de las Medidas de Seguridad Aplicables a los Datos Personales
Fase 3. Monitorear y Revisar el SGSDP	• **Paso 8.** Revisiones y Auditoría
Fase 4. Mejorar el SGSDP	• **Paso 9.** Mejora Continua y Capacitación

Elaboración del documento de seguridad

PASO 1

¿QUÉ DATOS PERSONALES TRATO?

INVENTARIO DE DATOS PERSONALES

¿Qué debe contener el documento que hace constar las medidas de seguridad?

Artículo 37. De manera particular, el responsable deberá elaborar 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, y

VII. El programa general de capacitación.

Paso 1 (Artículo 77, fracciones I, II y III)

Definición y diseño de las actividades de tratamiento

Es un paso fundamental, requiere tener claro cuáles son las finalidades del tratamiento de datos personales.

Cada sujeto obligado, de acuerdo al principio de responsabilidad proactiva (accountability), debe decidir el nivel de agregación o segregación para elaborar el registro de actividades de tratamiento y deberá valorar hasta qué punto esa agregación o segregación corresponde con finalidades, bases jurídicas y grupos de individuos distintos.

¿ Qué es el Inventario de datos personales?

- Control documentado, sobre los tratamientos de datos personales realizados por las unidades administrativas con orden y precisión.
- Los elementos que debe incluir el inventario de tratamientos de datos personales, se definen en la LGPDPPSO (Art. 33 Frac III) y los Lineamientos Generales (federal) (Art. 58).
- El diagnóstico se deberá elaborar por proceso o función sustantiva
- Es responsabilidad de cada unidad administrativa la información de los tratamientos declarada en el inventario.

Responsabilidad

Denominación del sujeto obligado

Área (unidad administrativa) que detenta la información dentro del sujeto obligado y que tiene facultades jurídicas para decidir sobre el tratamiento de los datos.

¿Cómo obtengo los datos personales?

Responsabilidad (Denominación del sujeto obligado)		
Área (unidad administrativa) que detenta la información dentro del sujeto obligado y que tiene facultades jurídicas para decidir sobre el tratamiento de los datos.	Categorías de personas físicas identificadas o identificables a quien corresponden los datos que son tratados	En caso de seleccionar la opción otro, especificar el medio de obtención.
Unidad de Transparencia	solicitantes	Directamente del titular
	Empleados	
	Proveedores	
	Solicitantes de información	
	Propietarios de bienes inmuebles	

¿Cómo obtengo los datos personales?

Medio de obtención de los datos personales (1)		
Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, se deberá indicar un medio por fila.	Describir el medio, por ejemplo la fuente de acceso público, URL, domicilio, número telefónico, entre otros	En caso de seleccionar la opción otro, especificar el medio de obtención.
De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Asesoramiento mediante CAS	N/A
Correo electrónico	Correos institucionales de cualquier servidor público del INAI	
Internet o sistema informático	PNT	
Escrito o formato presentado directamente en el INAI	Escrito presentado en Oficialía de Partes	
Escrito o formato enviado al INAI por mensajería	Escrito presentado en Oficialía de Partes	
Por transferencia	A través de los sujetos obligados con motivo de la sustanciación y organismo garante local	
Fuente de acceso público	Internet/ Registro público de propiedad y comercio/registro civil/	
Vía telefónica	Telinai	

* Es relevante para conocer cómo poner a disposición el aviso de privacidad

¿Qué datos personales trato?

Listado de datos personales (4)		Sensible (5)
Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	En caso de seleccionar la opción otro, especificar.	Señalar si el dato personal es sensible o no.
Datos de identificación		No
Datos personales contenidos en documento para acreditar personalidad del representante		No
Datos personales contenidos en la denuncia		Sí
Otro, especificar en la columna siguiente	Datos personales aportados en el contenido de la solicitud	Sí
Discapacidad		Sí
Circunstancias socioeconómicas		Sí
Lengua indígena		Sí
Otro, especificar en la columna siguiente	Datos de contacto	No
Estado de interdicción o incapacidad legal		Sí

¿Cómo los guardo?

Formato de la base de datos (6)	Ubicación base de datos (7)	
Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.	Señalar la ubicación de la base de datos. Si es más de uno, se deberá indicar uno por fila.	En caso de seleccionar la opción otro, especificar la ubicación.
Físico	Archiveros de la unidad administrativa	N/A
Electrónico	Equipo de cómputo	
	Servidor de la Institución	
	Archivo de concentración	

¿Cómo los organizo?

*** Debe guardar congruencia con los clasificadores empleados en materia archivística**

Sección de archivos (8)	Serie de archivos (9)	Subserie de archivos (10)
Indicar clave de identificación de la sección a la que corresponde el tratamiento.	Indicar clave de identificación de la serie a la que corresponde el tratamiento.	Indicar clave de identificación de la subserie a la que corresponde el tratamiento.
Ejemplo SC03S	*Ejemplo SE01*	*Ejemplo SS02*

Debemos atender al ciclo de vida de los documentos que tengan datos personales

Artículo 4. Para los efectos de esta Ley se entenderá por:

I…
XIV. Ciclo vital: A las etapas por las que atraviesan los documentos de archivo desde su producción o recepción hasta su baja documental o transferencia a un archivo histórico;
V. Archivo de trámite: Al integrado por documentos de archivo de uso cotidiano y necesario para el ejercicio de las atribuciones y funciones de los sujetos obligados;
IV. Archivo de concentración: Al integrado por documentos transferidos desde las áreas o unidades productoras, cuyo uso y consulta es esporádica y que permanecen en él hasta su disposición documental;
…
VIII. Archivo histórico: Al integrado por documentos de conservación permanente y de relevancia para la memoria nacional, regional o local de carácter público;
…
XII. Baja documental: A la eliminación de aquella documentación que haya prescrito su vigencia, valores documentales y, en su caso, plazos de conservación; y que no posea valores históricos, de acuerdo con la Ley y las disposiciones jurídicas aplicables;

Ley General de Archivos

Debe vincularse el tratamiento de los datos con los cuadros y catálogos

Artículo 4

XX. Cuadro general de clasificación archivística: Al instrumento técnico que refleja la estructura de un archivo con base en las atribuciones y funciones de cada sujeto obligado;

XIII. Catálogo de disposición documental: Al registro general y sistemático que establece los valores documentales, la vigencia documental, los plazos de conservación y la disposición documental;

XXXIX. Inventarios documentales: A los instrumentos de consulta que describen las series documentales y expedientes de un archivo y que permiten su localización (inventario general), para las transferencias (inventario de transferencia) o para la baja documental (inventario de baja documental);

La sección, serie y subserie debe ser idéntica en los inventarios de datos y en los catálogos

XXXIII. Fondo: Al conjunto de documentos producidos orgánicamente por un sujeto obligado que se identifica con el nombre de este último;

XLIX. Sección: A cada una de las divisiones del fondo documental basada en las atribuciones de cada sujeto obligado de conformidad con las disposiciones legales aplicables;

LV. Subserie: A la división de la serie documental;

L. Serie: A la división de una sección que corresponde al conjunto de documentos producidos en el desarrollo de una misma atribución general integrados en expedientes de acuerdo a un asunto, actividad o trámite específico;

XXIX. Expediente: A la unidad documental compuesta por documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados;

XXX. Expediente electrónico: Al conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan;

XXIV. Documento de archivo: A aquel que registra un hecho, acto administrativo, jurídico, fiscal o contable producido, recibido y utilizado en el ejercicio de las facultades, competencias o funciones de los sujetos obligados, con independencia de su soporte documental;

Ley General de Archivos

¿Para qué trato los datos?

*** Debe coincidir plenamente con lo expresado en el aviso de privacidad**

	Finalidades del tratamiento (11)
	Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una por fila.
Finalidades Primarias	dar atención a la denuncia
	Realizar las investigaciones conducentes
Finalidades secundarias	fines estadísticos

Consentimiento

¿Requiere consentimiento? (12)	Supuesto artículo 18 que se actualiza, en su caso (13)	Tipo de consentimiento (14)
Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad no requiera el consentimiento del titular, señalar el o los supuestos del artículo 22 de la LGPDPPSO que se actualizan.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.
No	I	Tácito
Sí	IV	Expreso

Excepciones al principio de consentimiento

Artículo 19. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley en ningún caso podrán contravenirla;

II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o

X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en materia.

¿Quién trata los datos personales dentro de la organización?

* Es relevante para las medidas de seguridad

Servidores públicos que tienen acceso a la base de datos (15)	Área de adscripción (16)	Finalidad del acceso (17)	Función o atribución que justifica el acceso (18)
Señalar los puestos (cargos o nombramientos) de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Incluir el nombre	Definir unidad administrativa a la que está adscrito el puesto	Señalar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.	Señalar la atribución que faculta a la persona a acceder a los datos personales.

¿Quién trata los datos personales fuera del sujeto obligado?

Nombre del encargado, en su caso (19)	No. de contrato, pedido o convenio con el encargado, o del instrumeto jurídico correspondiente (20)
Señalar nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso. Uno por fila.	Señalar el número de identificación del instrumento jurídico que regula la relación con el encargado.
Ejemplo Grupo de Tecnología Cibernética	1777757

* Establecer mecanismos para garantizar la protección de datos personales
* Precisar en qué momento se dará a conocer el aviso de privacidad o incluirlo en el contrato.

¿Con quien comparto la información fuera del sujeto obligado?

* Debe guardar congruencia con el aviso de privacidad

¿Se realizan transferencias? (21)	Tercero al que se transfieren los datos personales, en su caso (22)	Finalidades de la transferencia (23)	¿Requiere consentimiento la transferencia? (24)
Señalar si se realizan o no transferencias en el marco del tratamiento.	Señalar el nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, cuando ello sea posible, o bien, su categoría. Uno por fila.	Señalar las finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.	Señalar si la transferencia requiere o no consentimiento.

¿Con quien comparto la información fuera del sujeto obligado?

* Debe guardar congruencia con el aviso de privacidad

Supuestos artículos 22, 66 o 70 LGDPPSOque se actualizan, en su caso (25)	**Tipo de consentimiento que se requiere para la transferencia (26)**	**¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico? (27)**	**Supuesto artículo 66 que se actualiza, en su caso (28)**
En caso de que la transferencia no requiera consentimiento, señalar los supuestos que se actualizan.	En caso de que la finalidad de la transferencia requiera el consentimiento del titular, señalar si se requiere el tácito o el expreso y por escrito.	Indicar si la transferencia requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, según el artículo 66 de la LGPDPPSO.	Señalar el supuesto que en su caso se actualiza, si no se requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico.

Conceptos

Remisión:
Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

Transferencia:
Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

Transmisión:
Toda comunicación de datos personales realizada entre el responsable transmisor y el responsable receptor, a partir de la portabilidad de datos personales. Tratándose de servicios de cómputo en la nube, la comunicación de datos personales de un servicio o aplicación de un responsable a otro.

¿Hay datos que se hacen públicos?

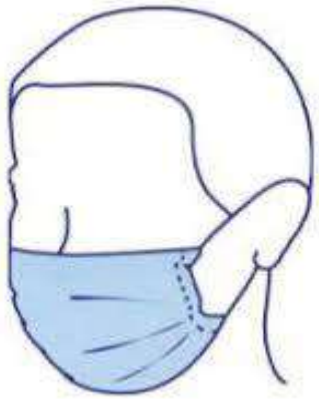
Difusión de los datos personales (28)	Datos personales objeto de difusión	Fundamento jurídico para la difusión (29)
Indicar si en el tratamiento se realiza la difusión de los datos personales.	Indicar los datos personales que son difundidos	Indicar el fundamento jurídico que ordena la difusión de los datos personales.
No		N/A
Sí	Nombre Cargo Sueldo	

Plazo de conservación (30)	Bloqueo (31)	Observaciones
Señalar el plazo de conservación de los datos personales, según lo señalado en los instrumentos de clasificación archivística.	Precisar el periodo de bloqueo al que se sujetarán los datos en caso de ejercicio de derecho de Cancelación	Espacio libre para hacer aclaraciones y precisiones
Permanente		

La normatividad parte de un modelo de gestión de riesgos

Las medidas de seguridad son proporcionales a los riesgos que se enfrentan

ANÁLISIS DE RIESGO



¿Qué es la gestión de riesgos?

Es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación.

Se puede dividir en tres etapas diferenciadas:

1. La identificación
2. La evaluación y
3. El tratamiento de los riesgos.

Identificar amenazas y riesgos

Riesgo: la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo.

Amenaza: cualquier factor de riesgo con potencial para provocar un daño o perjuicio.

Tipos de amenazas

- Acceso ilegítimo a los datos
- Modificación no autorizada de los datos
- Eliminación o pérdida de los datos

Evaluar los riesgos

- Consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice.
- El impacto, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se materializa.

La evaluación se hace considerando el daño a los titulares de los datos personales, no de los sujetos obligados.

¿Cómo identificar y gestionar los riesgos potenciales asociados a una actividad de tratamiento?

Los riesgos son variables y dependen de las amenazas a las que está expuesta la actividad de tratamiento, por ello, es fundamental disponer de una descripción detallada del tratamiento, de su contexto y de los elementos más relevantes que intervienen en la misma

¿Riesgo para qué y para quién?

Distinguir claramente

1. el riesgo del tratamiento para la persona y
2. el riesgo de incumplimiento para quien trata los datos personales.

Evaluar el riesgo (II)

- Caso por caso:
  - Factores o circunstancias a considerar (naturaleza de los datos personales, quiénes son los titulares de los datos personales, etc.).
  - Medidas adoptadas o brechas en las medidas.
  - Otras acciones por quien trata los datos personales (consultas previas, diligencia o cuidado, etc.).

¿Quién tiene que identificar el riesgo?

- Quien trata los datos personales, ya sea responsable o encargado del tratamiento.
- Considerar cuándo es obligatorio o recomendable (siempre)?
- ¿Qué nivel de conocimiento sobre riesgos tiene quién los identifica?
- ¿Qué nivel de riesgo asume quien trata los datos personales? ¿Cómo es su programa de protección de datos y qué medidas ha adoptado?

Análisis de Riesgo de los Datos Personales

Factores para determinar las medidas de seguridad

Nos ayudan a definir…

Criterios de Evaluación del Riesgo

- Paso 1. Alcances y Objetivos
- Paso 2. Política de Gestión de DP
- Paso 3. Funciones y Obligaciones
- Paso 4. Inventario de DP

Criterios de evaluación

CRITERIOS DE EVALUACIÓN

Tolerancia máxima

Impacto

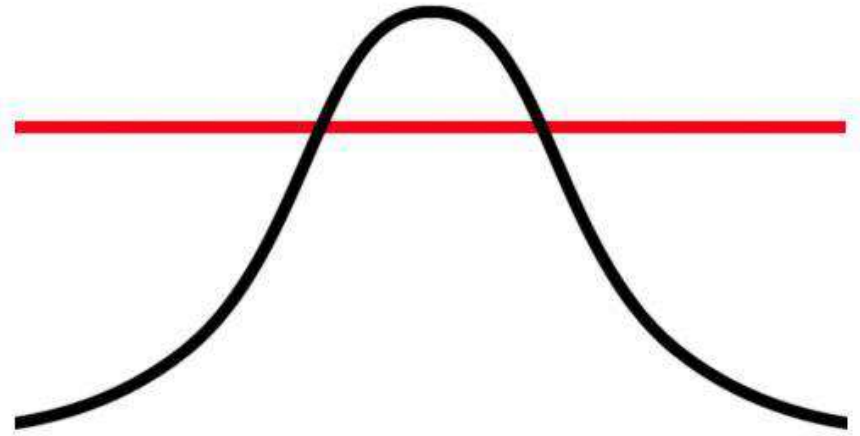
Aceptación

Daño a los titulares

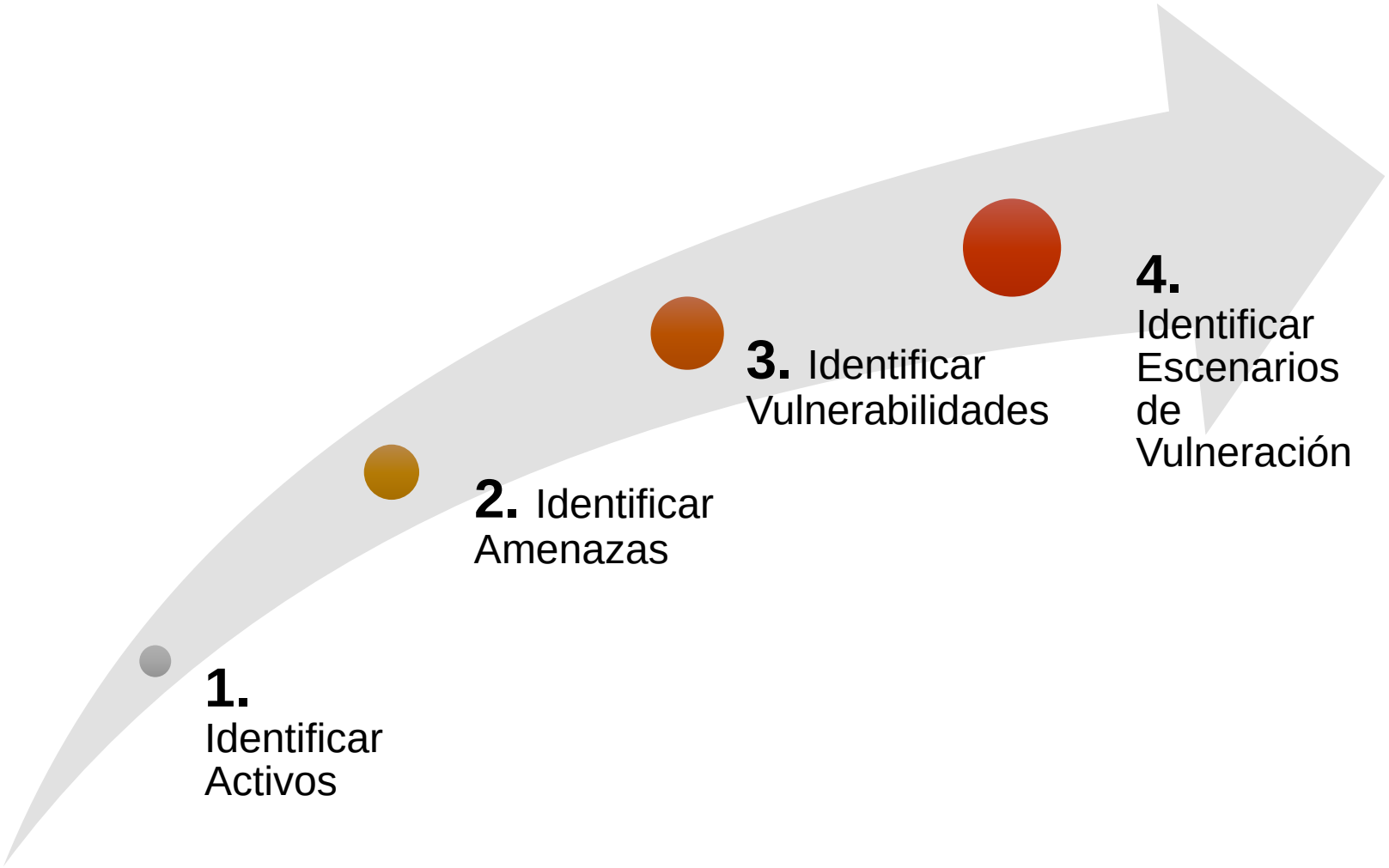
Daño a la organización

Criterios de evaluación del riesgo

- Criterio de Impacto:
  - No contar con medidas de seguridad óptimas en sus sistemas de tratamiento para datos sensibles.
- Criterio de Aceptación:
  - No tener un Aviso de Privacidad correcto.



Valoración respecto al riesgo



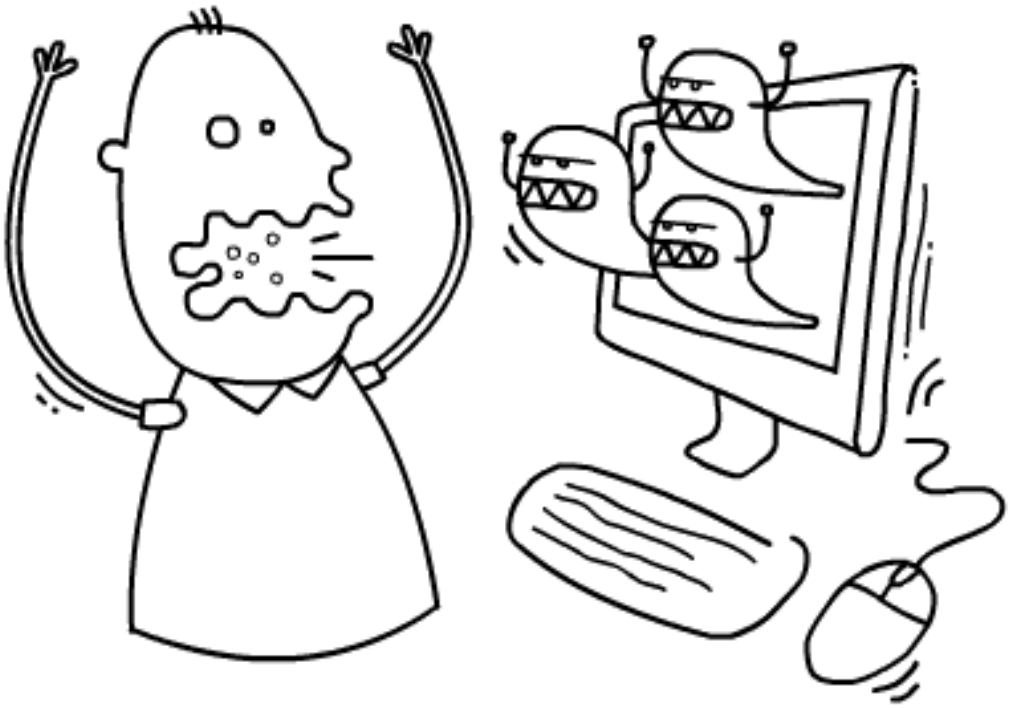
Activos de Información

Activos de Apoyo

1. Identificación de Activos

Empleados Prospectos

Pacientes



Una **amenaza** tiene el potencial de dañar un activo.

Pueden ser de origen natural o humano, accidentales o deliberadas y además provenir de adentro o fuera de la organización.

2. Amenazas de los Activos

Fuego

Virus

Las **vulnerabilidades** son *debilidades en los activos*

3.Vulnerabilidades de los Activos

Material susceptible al fuego

Falta de antivirus

ACTIVO	AMENAZA	VULNERABILIDAD	DAÑO/IMPACTO	POTENCIAL/PROBABILIDAD
Aquiles	Guerra de Troya	Talón	Muerte	Muy probable

Expediente de Paciente (electrónico)	Virus	Computadoras sin antivirus	Borrado permanente de información	Muy probable
ACTIVO	**AMENAZA**	**VULNERABILIDAD**	**DAÑO/IMPACTO**	**POTENCIAL/PROBABILIDAD**
Expediente de Paciente (papel)	Incendio	Material susceptible al fuego	Pérdida definitiva de información	Poco probable

DESCRIPCIÓN DEL TRATAMIENTO			
Su propósito	**Su naturaleza**	**Su ámbito/ alcance[46]**	**Su contexto**
• Fines últimos. • Fines instrumentales. • Fines secundarios. • Otros…	• Las etapas en las que se implementa. • El flujo de datos personales. • Las operaciones de tratamiento que precisa (manuales y automatizadas). • Los activos/ elementos sobre los que se implementa. • Los roles que acceden a los datos. • Las características tecnologías relevantes. • La participación de encargados en distintas	• La extensión en la cantidad de datos. • La extensión en la cantidad de sujetos afectados. • La extensión en los tipos y categorías de datos. • La extensión geográfica. • La extensión en el tiempo del tratamiento. • La extensión en el tiempo de la conservación. • La frecuencia de recogida. • La granularidad. • Otros…	• El mercado o sector en el que se desenvuelve. • El entorno social en el que despliega. • El entorno normativo. • La interacción con otros tratamientos de la entidad. • Las cesiones de datos que son necesarias. • Las transferencias internacionales que implica. • Las brechas de seguridad o incidentes que se producen en tratamientos

https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

No.	Nombre del activo	Ubicación	Tipo de Activo
1	Nombre de la persona fisica. Primer Apellido, Segundo Apellido, Correo Electrónico y Telefono Celular	DGPAR	Información
2	Oficios	Archivero	Apoyo
3	Nombre de la persona fisica. Primer Apellido, Segundo Apellido, Correo Electrónico y Telefono Celular	carpeta compartida	Apoyo
4	Sistema X	servidor	Apoyo

Categoria del Activo	Subcategoria	Valor cualitativo	Propietario del activo	Custodio del activo
Datos_Personales	Personales de Identificación	Medio	DGPAR	Dirección de Facilitación Sector Privado
TICs_comunicaciones_y_demás_equipamiento	Computadoras de escritorio	Bajo	Dirección de Facilitacion del Sector Privado	Dirección de Facilitación Sector Privado
TICs_comunicaciones_y_demás_equipamiento	Sistema de Archivos Compartidos	Alto	Dirección de Facilitacion del Sector Privado	DGTI
Aplicaciones_y_bases_de_datos	Software de sistemas	Alto	Unidad de Transparencia	DGTI

Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo	
				Cuantitativo	Cualitativo
Modificación accidental de datos	Inadecuado nivel de conocimiento y/o concienciación de empleados	1	2	2	Bajo
Errores de aplicaciones / software	Falta de control en datos de entrada y salida	3	2	6	Alto

Evaluación del riesgo	Propietario del riesgo	Controles existentes (antes de su tratamiento)	Nivel de madurez de los controles existentes	D
Riesgo aceptable	Direccion de Facilitacion del Sector Privado	Bitácora de Control de Acceso (Administrativo)	2. Se aplica, esta documentado y formalizado	
Riesgo no aceptable	DGTI	Procedimiento de desarrollo	1. Se aplica sin estar documentado ni formalizado	

Sanción al servidor público.
Multas no pagables con recursos públicos.
¿Reparación del daño al afectado?

Determinación del nivel de madurez de los controles existentes	Opción de tratamiento	Controles de seguridad para el tratamiento
El riesgo no tiene que ser tratado		• Seguridad de servicios de red
El riesgo debe ser tratado	1. Reducir el riesgo	14.1.1 Análisis y especificación de requisitos de seguridad

Anexos que dan cuenta de las medidas de seguridad.
Por ejemplo, tipo de software usado, uso de mecanismos de identificación y autenticación, etc

Impacto	Probabilidad	Riesgo		Evaluación del riesgo (riesgo residual)
		Cuantitativo	Cualitativo	
2	1	2	Bajo	Riesgo aceptable

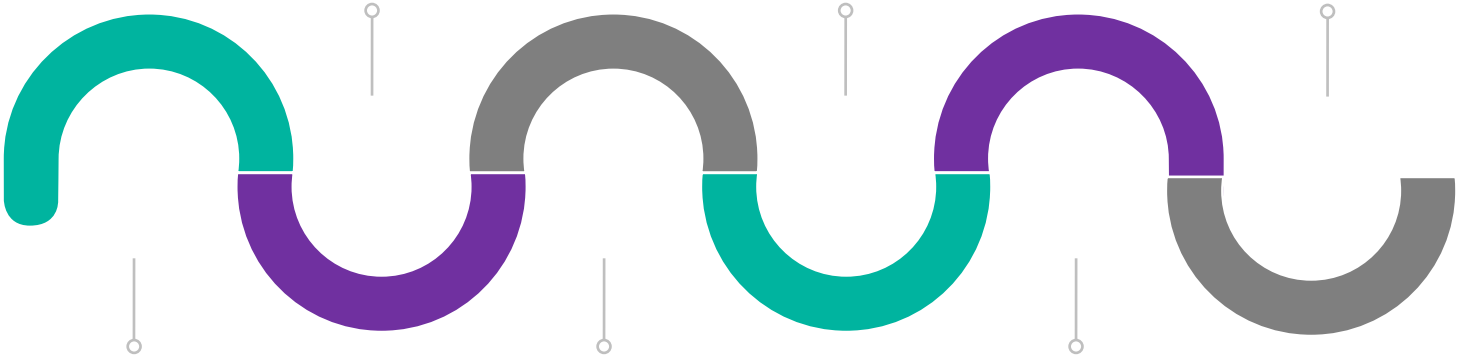
Decisión del responsable en relación al costo-beneficio

Fase 1

Paso 2. Política de Gestión de DP

Paso 4. Inventario de DP

Paso 6. Análisis de Brecha



Paso 1. Alcances y Objetivos

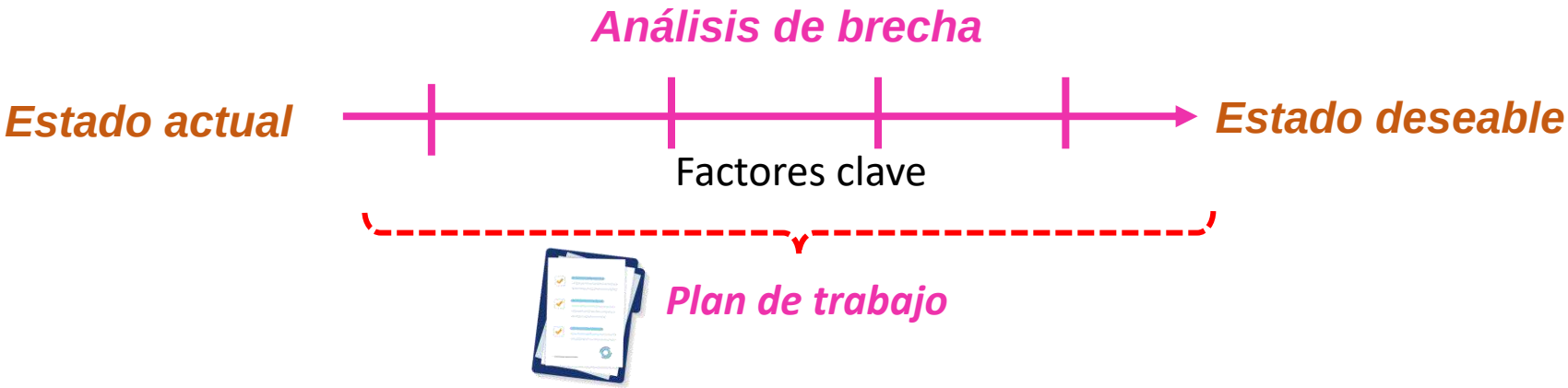
Paso 3. Funciones y Obligaciones

Paso 5. Análisis de Riesgo de DP

IV. Análisis de brecha

El **análisis de brecha** consiste en 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.

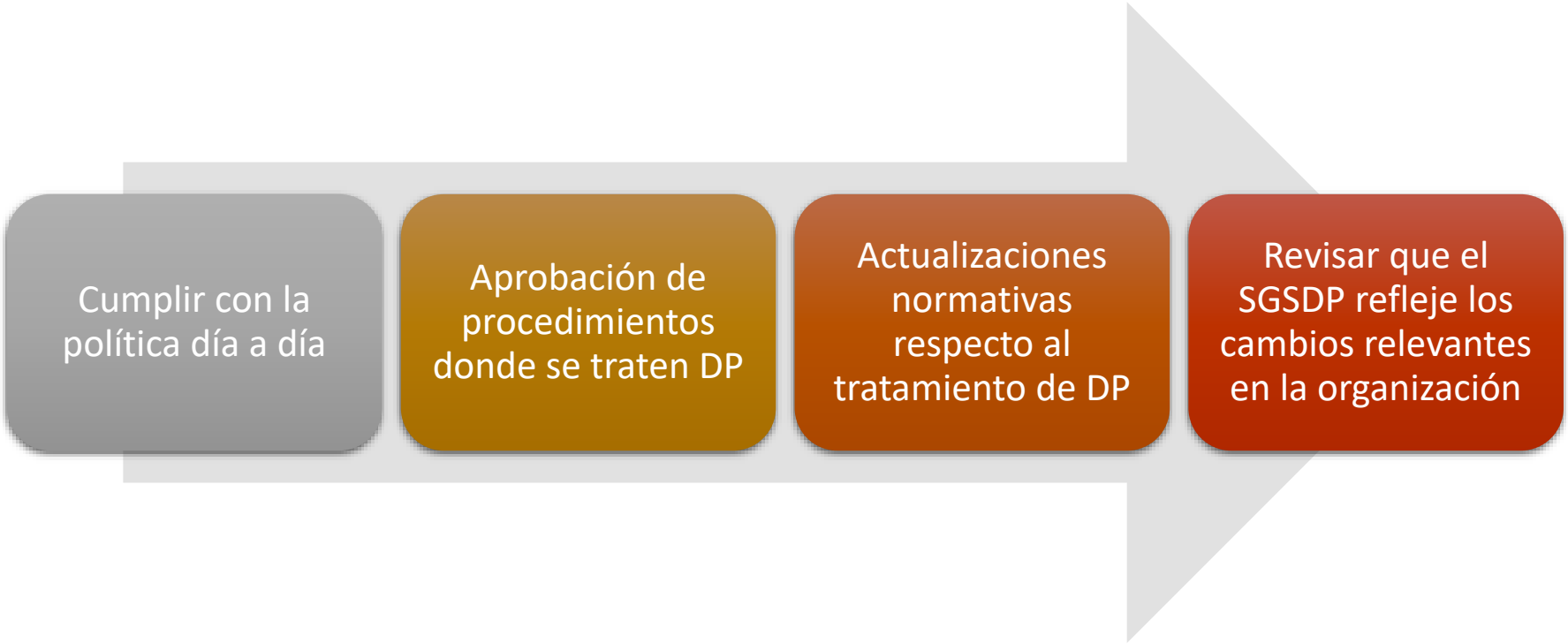


Implementación de las Medidas de Seguridad Aplicables a los Datos Personales

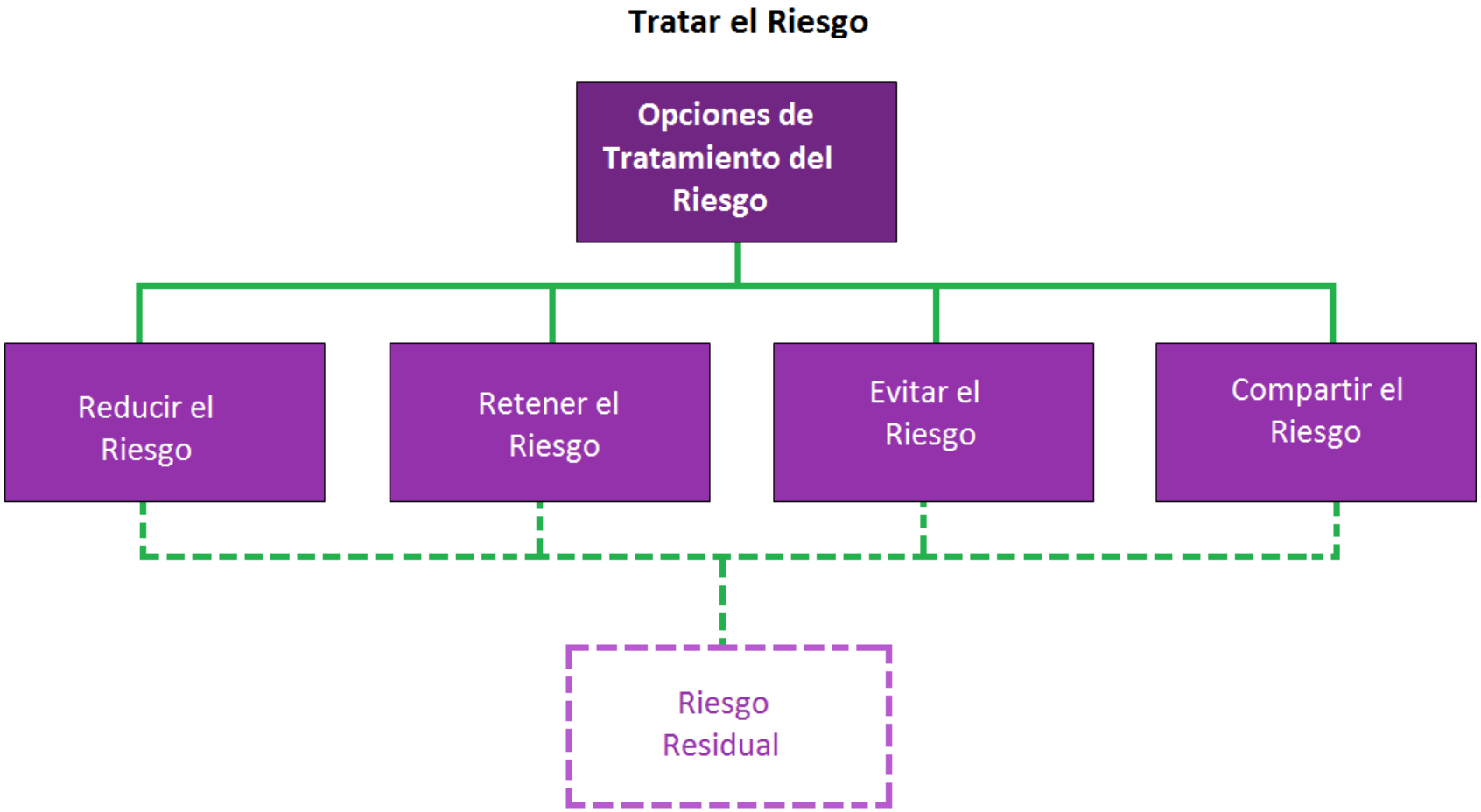
Cumplimiento Cotidiano de Medidas de Seguridad

Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes

Cumplimiento Cotidiano de Medidas de Seguridad



Tratamiento del riesgo



Reducir

- **Reducir el Riesgo.** Corrección, eliminación, prevención, minimización del impacto, disuasión, recuperación, monitoreo y concienciación.

Retener

- **Retener el Riesgo.** No hay necesidad inmediata de implementar controles adicionales.

Evitar

Evitar el Riesgo. Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios.

Compartir

Compartir el Riesgo. Un tercero interviene para mitigar los posibles efectos de un riesgo.

Aceptar

Aceptar el Riesgo. Asumir formalmente las decisiones sobre el plan de tratamiento del riesgo.

Relación de tablas de la guía de Gestión del riesgo y ...
https://www.aepd.es › documento › relacion-tabla.

FASE 3: MONITOREAR Y REVISAR EL SGSDP

Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** Elaborar un Inventario de Datos Personales • **Paso 5.** Realizar un Análisis de Riesgo de Datos Personales • **Paso 6.** Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	• **Paso 7. Implementación** de las Medidas de Seguridad Aplicables a los Datos Personales
Fase 3. Monitorear y Revisar el SGSDP	• **Paso 8. Revisiones y Auditoría**
Fase 4. Mejorar el SGSDP	• **Paso 9.** Mejora Continua y Capacitación

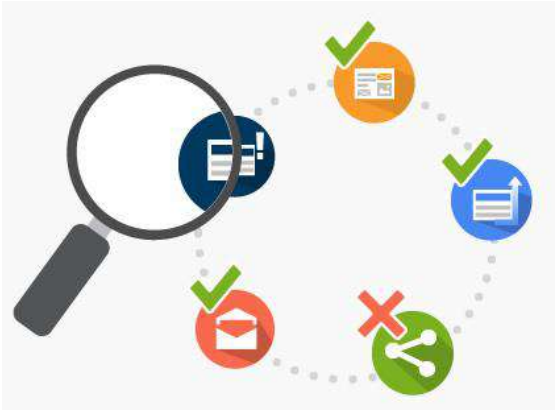
Paso 8. Revisiones y Auditoría

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

Revisión de los factores de riesgo

Auditoría

Vulneraciones a la Seguridad de la Información



Vulneraciones a la seguridad

- Robo
- Pérdida
- Acceso
- Daño

Acciones en caso de vulneración a la seguridad

1) Identificación de la vulneración

2) Notificación de la vulneración

3) Remediación del incidente

* Deben llevarse bitácoras de vulneración.

FASE 4: MEJORAR EL SGSDP

Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** Elaborar un Inventario de Datos Personales • **Paso 5.** Realizar un Análisis de Riesgo de Datos Personales • **Paso 6.** Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	• **Paso 7. Implementación** de las Medidas de Seguridad Aplicables a los Datos Personales
Fase 3. Monitorear y Revisar el SGSDP	• **Paso 8. Revisiones y Auditoría**
Fase 4. Mejorar el SGSDP	• **Paso 9. Mejora Continua y Capacitación**

Paso 9. Mejora continúa y capacitación

Acciones correctivas

Acciones preventivas

Capacitación

VII. Programa general de capacitación en materia de datos personales

- Concienciación
- Entrenamiento
- Educación

Cuida los datos personales
que tratas
como si los fueran tuyos

@INAImexico
@OscarGuerraFord
@gimontes

inaimexico

Lecturas de apoyo recomendadas

Herramientas de apoyo del INAI

Para cumplir con las medidas de seguridad

1. **Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (Octubre, 2013).**
http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementaci%C3%B3n_SGSDP_ene2014.pdf

2. **Tabla de Equivalencia Funcional entre estándares de seguridad, la LFPDPPP, su Reglamento y recomendaciones en la materia (Mayo, 2014).**
http://inicio.ifai.org.mx/DocumentosdeInteres/Tabla_Equivalencia_Funcional_2014.pdf

3. **Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas (Julio, 2014).**
http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf

4. **Manual en materia de seguridad de los datos personales y otra información basada en un entorno Microsoft para MIPYMES y organizaciones pequeñas mexicanas (Microsoft). (Diciembre, 2015)**
http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Microsoft.pdf

Herramientas de apoyo del INAI

Para cumplir con otras obligaciones

Guía para cumplir con los principios y deberes de la LFPDPPP (Julio, 2014).

http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20obligaciones%20de%20la%20LFPDPPP.pdf

Guía para Prevenir el Robo de Identidad (Enero, 2016)

http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf

Guía para instrumentar medidas compensatorias (Marzo, 2014).

http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf

Guía para orientar el debido tratamiento de datos personales en la actividad de cobranza extrajudicial (Diciembre, 2014).

http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20Cobranza%20Extrajudicial%20IFAI.pdf

Fuentes

- Merriam-Webster Dictionary, disponible en https://www.merriam-webster.com/dictionary/cyber.
- ISO/IEC 27032 Guidelines for cybersecurity, disponible en https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.
- European Union, “Help: Glossary | Europa – Information Society ‘C’, disponible en http://ec.europa.eu/ information_society/tl/help/glossary/index_en.htm#c.
- United States, National Security Presidential Directive 54/Homeland Security Presidential Directive 23, 2008, disponible en http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
- ISO/IEC 27032 Guidelines for cybersecurity, disponible en https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

Fuentes

- The Netherlands, The National Cyber Security Strategy, 2011, disponible en http://english.nctb.nl/Images/cyber-security-strategy-uk_tcm92-379999.pdf.

- http://www2.scjn.gob.mx/AsuntosRelevantes/pagina/SeguimientoAsuntosRelevantesPub.aspx?ID=139112&SeguimientoID=575&CAP=

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS (LPPDPPSO)

http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Programa de Protección de Datos

Documento Orientador

http://inicio.inai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m4

FORMATO DE AUTOEVALUACIÓN DE AVISOS DE PRIVACIDAD

http://inicio.inai.org.mx/SitePages/Aviso-Privacidad.aspx

- SO/IEC 27005:2008 Tecnologías de la Información – Técnicas de Seguridad – Gestión de riesgos de seguridad de la Información.
- ISO 31010 de Gestión y Evaluación de Riesgos
- ISO 29134 Tecnologías de la información – Guías para las Evaluaciones de Impacto en la Protección de los Datos WP248
- Guía sobre las Evaluaciones de Impacto en Protección de datos – Grupo Europeo Artículo 29


Gracias