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

TALLER MEDIDAS DE SEGURIDAD SECTOR PÚBLICO

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES – PARTE 1

SECTOR PÚBLICO 2018

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

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN

Armando Becerra *@CiberArmand*

Noemi González *@nkglez*

¡Bienvenido a tu Taller!

Horario del taller: 13:15 a 15:15 hrs

Taller dividido en 2 partes

Agenda:

- Deber de Seguridad
- Importancia de la seguridad de los datos personales
- Publicaciones en materia de seguridad del INAI
- Definiciones útiles
- Implementación de un SGSDP – Caso IMA

Deber de Seguridad

Para garantizar la confidencialidad, integridad y disponibilidad de los datos personales:

- **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.**

¿Por qué me debe interesar la seguridad de los datos personales?

- La protección de datos personales es un derecho humano.
- Ayuda a mitigar los efectos de una vulneración a la seguridad.
- Evita daños a la reputación e imagen de la organización.
- Evita sanciones a los servidores públicos.

Sección de Seguridad de los Datos Personales

Publicación de documentos, y otras referencias respecto al deber de seguridad

DEFINICIONES

Definiciones de Ley General

Tratamiento

Medidas de seguridad

Base de datos

Sistema de Tratamiento

Activo

Cualquier recurso involucrado en el tratamiento de los datos personales, **que tenga valor para la organización.**

- ✓ **Activos de Información**
- ✓ **Activos de Apoyo**

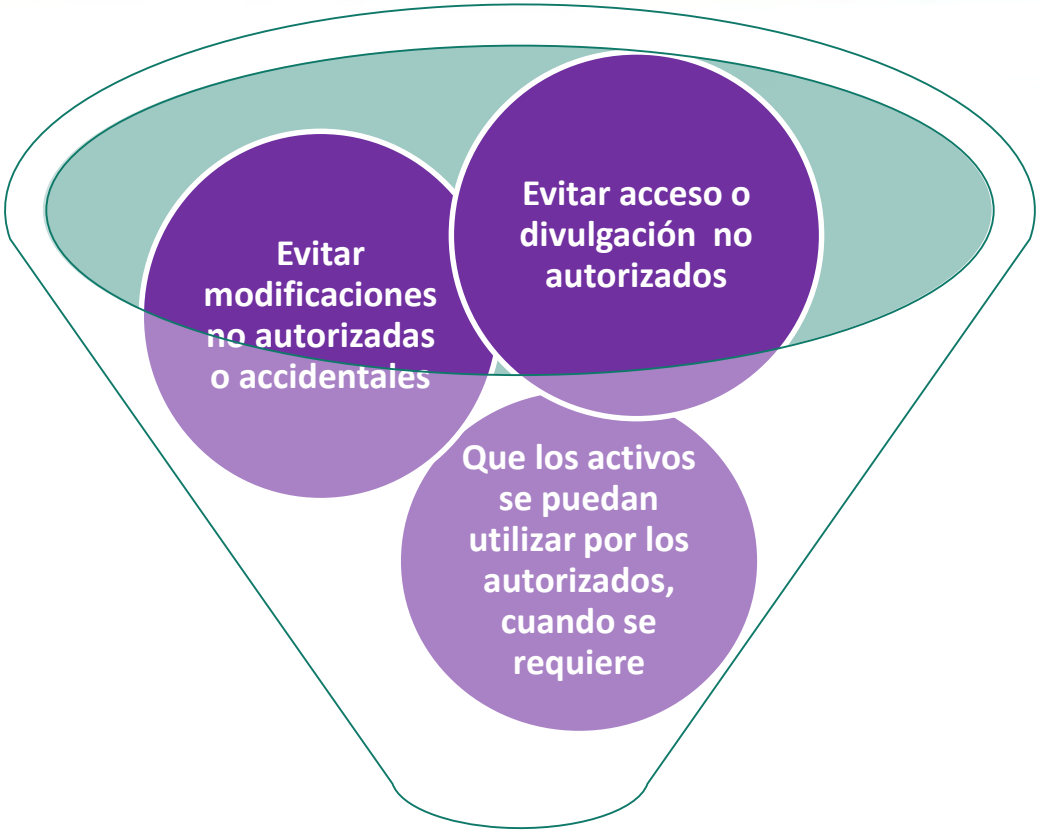
Alta Dirección

Toda persona **con poder legal** de toma de decisión en **las políticas de la organización.**

Custodio

Toda persona **con responsabilidad funcional sobre los activos.**

Seguridad de la Información



Preservar la **confidencialidad, integridad** y **disponibilidad** de los **activos**

Integridad

La propiedad de salvaguardar **la exactitud y completitud de los activos.**

- Evitar la modificación no autorizada o accidental.

Confidencialidad

Propiedad de la **información** para **no estar a disposición o ser revelada** a personas no autorizadas.

Prevenir la divulgación no autorizada de información.

Disponibilidad

Propiedad de un **activo** para ser **accesible y utilizable**.

- Controlar las interrupciones de los recursos.
- Prevenir interrupciones no autorizadas.

En resumen…

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

IMPLEMENTACIÓN DE UN SGSDP

Actividades mínimas para la seguridad de los datos personales

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

- Políticas gestión y tratamiento de datos personales
- Capacitación basada en niveles
- Funciones y obligaciones del personal que trata datos personales
- Monitoreo y revisión periódica medidas seguridad
- 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

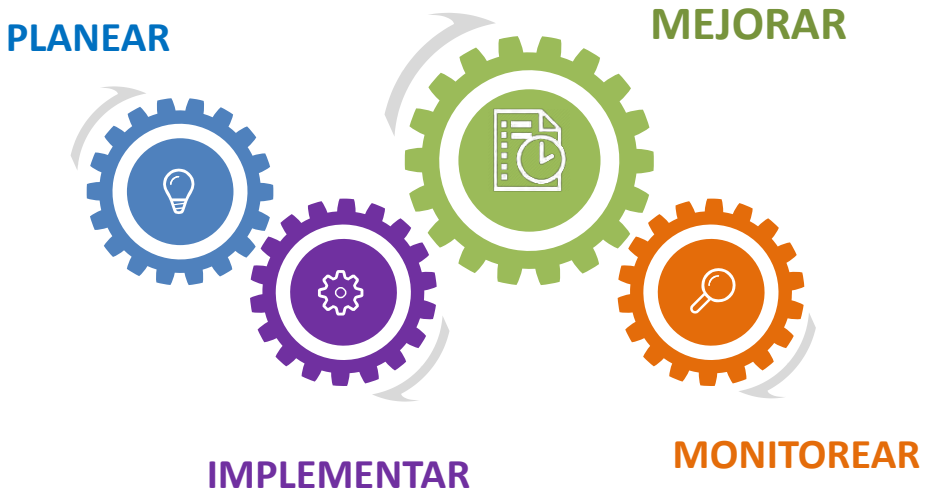
Artículo 33 de la LGPDPPSO

Sistema de Gestión de Datos Personales

Artículo 34 de la LGPDPPSO

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

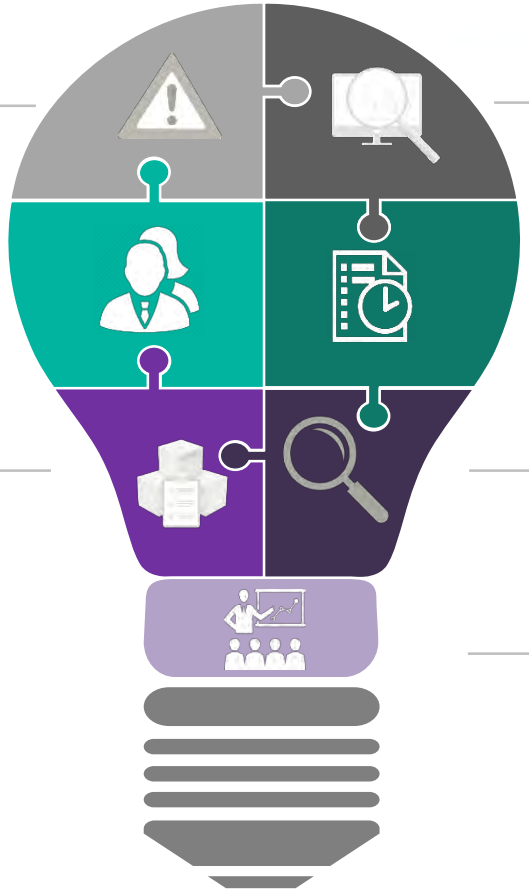


Documento de seguridad

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

Artículo 35 de la LGPDPPSO

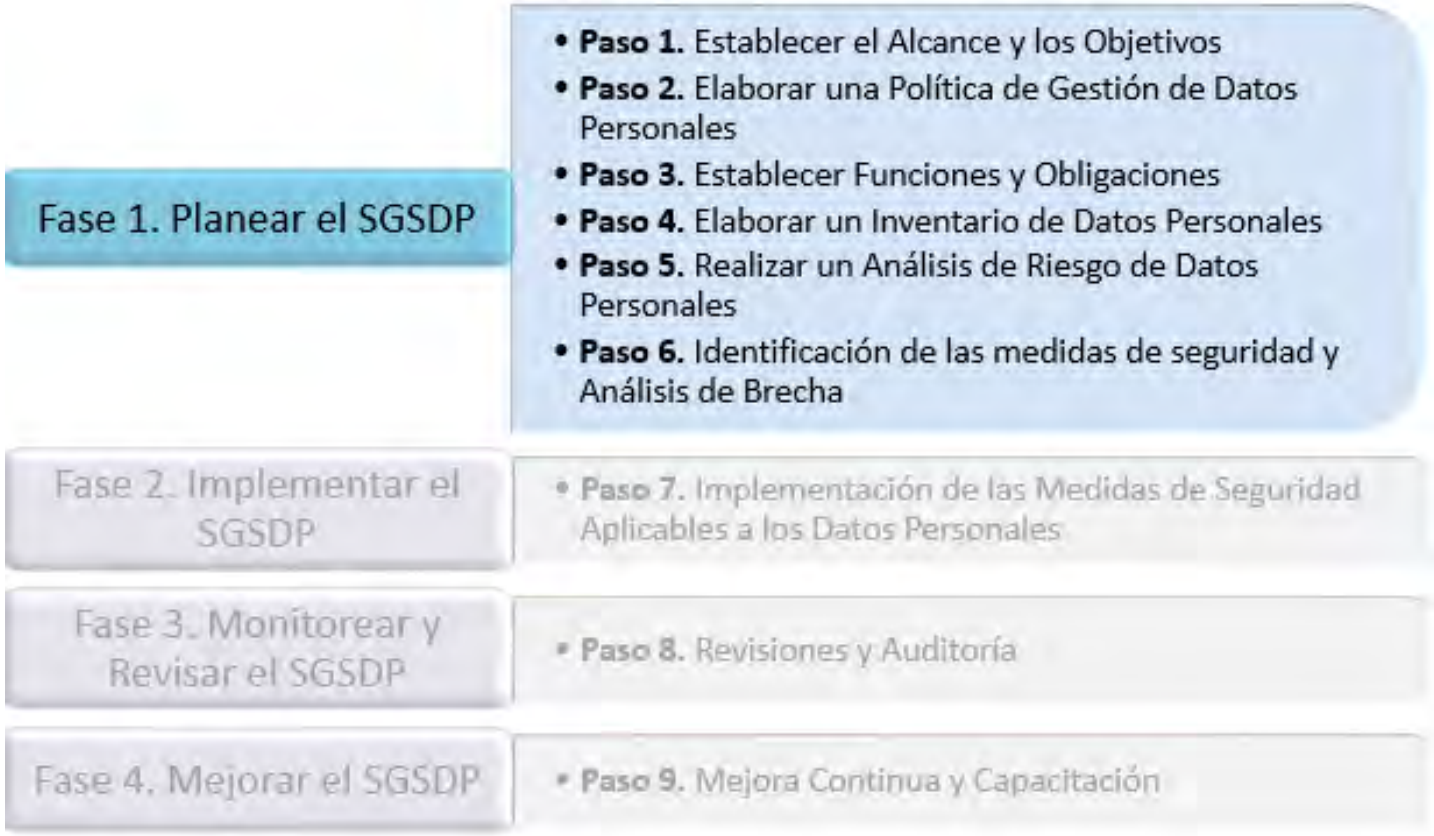
Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

DS

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

Caso de estudio: Instituto Mexicano de Audición (IMA)



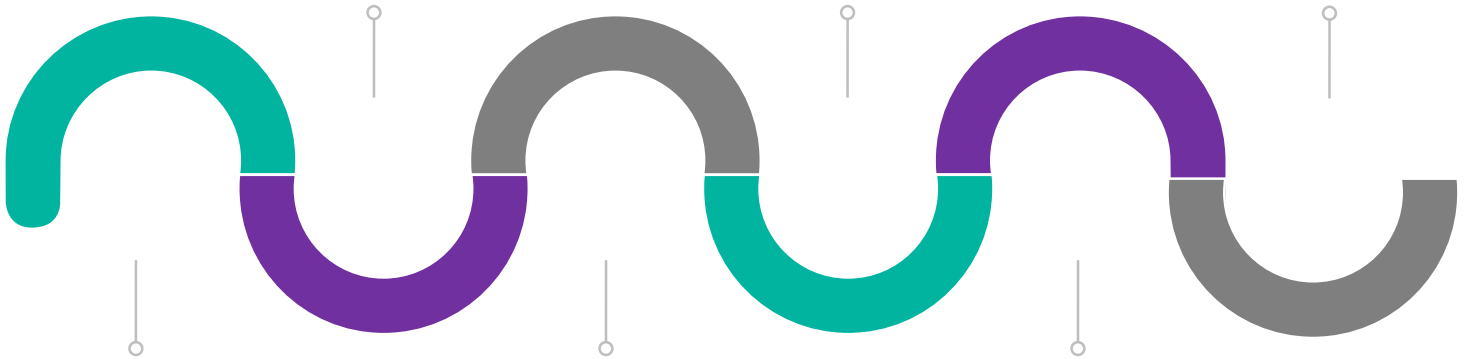
FASE 1: PLANEAR EL SGSDP

Fase 1

Paso 2. Política de Gestión de DP

Paso 4. Inventario de DP

Paso 6. Análisis de Brecha



Paso 1. Alcances y Objetivos

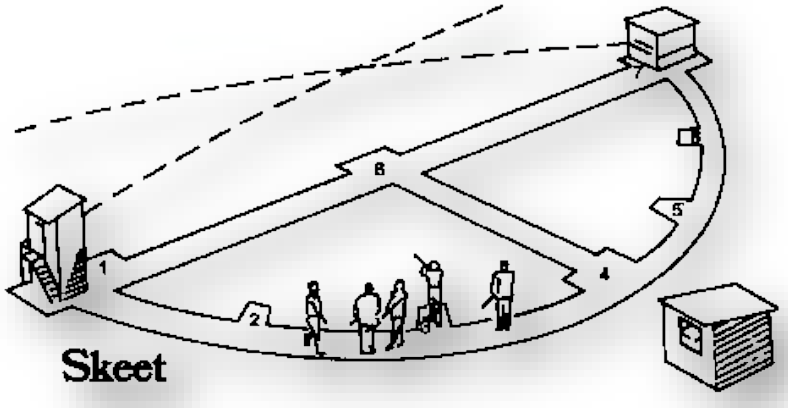
Paso 3. Funciones y Obligaciones

Paso 5. Análisis de Riesgo de DP

Paso 1. Establecer el Alcance y los Objetivos

Alcance

¿Hasta donde queremos llegar?



Objetivo

¿Qué se quiere lograr?

Paso 1. Establecer el Alcance y los Objetivos

- Factores contractuales
- Factores legales y regulatorios
- Factores del modelo de negocio
- Factores Tecnológicos

Factores contractuales

Entrega datos personales de identificación al personal del área de registro

Paciente (Titular)

Los **recibe** para otorgarle el servicio de audiometría.

Personal del área de donaciones (Responsable)

Recibe el resultado de la audiometría.

Entrega el resultado de la audiometría consentida por el paciente.

Manos a la obra

Ejercicio 1: Factores contractuales del IMA

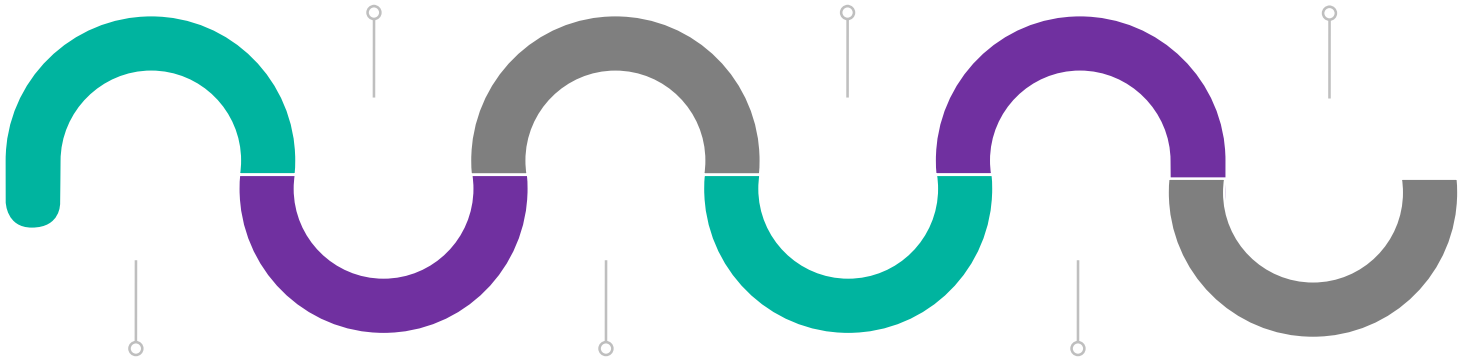
Actores	¿Quiénes son los actores involucrados en el Instituto Mexicano de Audición?
Titular (es)	Pacientes, Prospectos, Empleados
Responsable (s)	Instituto Mexicano de Audición/Director General
Encargado (s)	PubliDatos
Custodio (s)	Administrador 1, Administrador 2, Técnicos en Audiometría, Administrador de Donaciones
Alta gerencia	Director General, Subdirector de Recursos Humanos, Subdirector de Donaciones

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

Paso 2. Elaboración de 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**	**Tratamiento**	**Acción**	**Periodo de conservación**
Los Datos Personales	Recabados a través de formularios en papel	Por los técnicos de Audiometría	Para gestionar las donaciones	Deben ser destruidos	Después de un mes



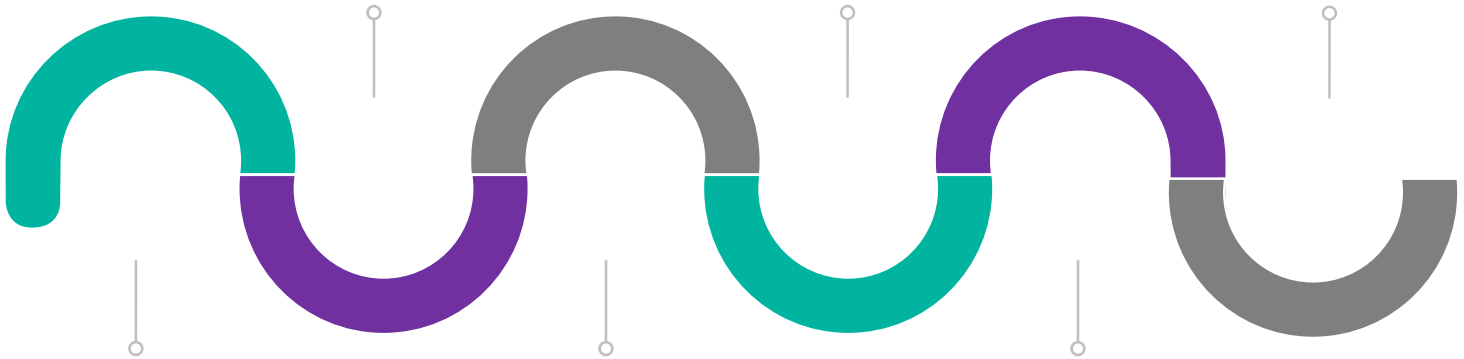

Fuente: *Technical Writing for IT Security Policies in Five Easy Steps, SANS Institute, InfoSec Reading Room.*

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

Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales

Recursos para que el SGSDP sea parte de la organización

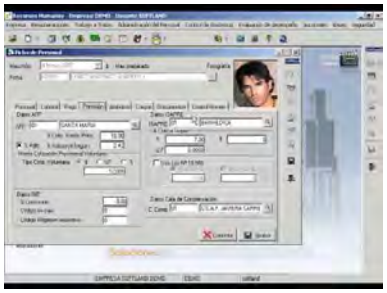
- Comunicar a todos los involucrados
- Roles y responsabilidades
- Contribución y consecuencias de incumplimiento

Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales

Actividades	Área de la Organización							
	Dirección y Gestión	Finanzas, Contabilidad y Ventas	Recursos Humanos	TIC	Área Legal	Auditoría Interna	Terceros	Infraestructura
Política y Objetivos del SGPDP	●	●	●	●	●			
Funciones y Obligaciones de Quienes Traten Datos Personales	●	●	●	●	●	●	●	●
Inventario de Datos Personales	●	●	●	●		●	●	●
Análisis de Riesgo de los Datos Personales	●	●	●	●	●	●	●	●
Análisis de Brecha de las Medidas de Seguridad		●	●	●	●	●	●	●
Implementación de las Medidas de Seguridad Aplicables a los Datos Personales	●	●	●	●	●	●	●	●
Revisiones y Auditoría						●		
Capacitación	●	●	●	●	●	●	●	●

Ejemplo: Funciones y obligaciones en IMA

	Obtención	Uso	Divulgación	Almacenamiento	Bloqueo	Cancelación
Sistema de Administración de personal	X	X			X	X
Archivero expedientes empleados		X		X		X

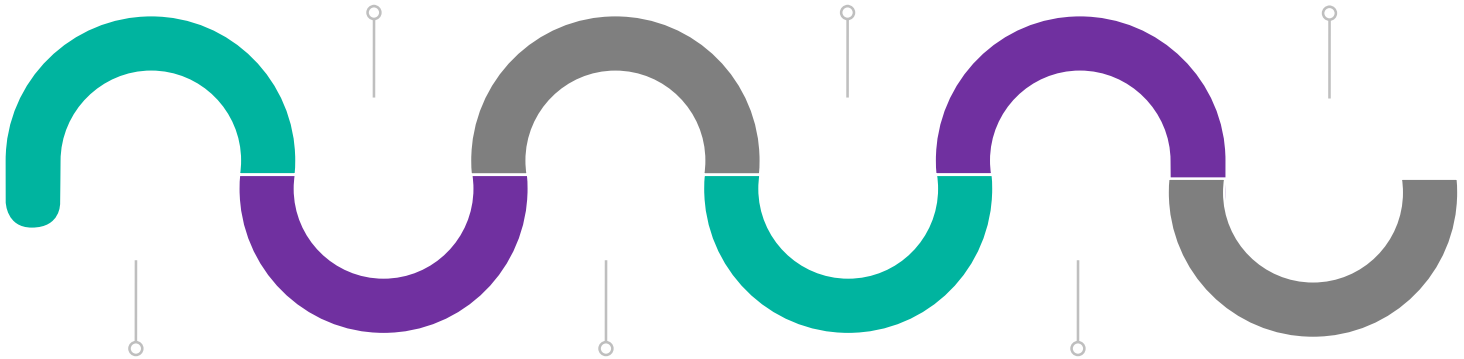


Fase 1

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

Paso 4. Inventario de datos personales

Ciclo de vida de los Datos Personales

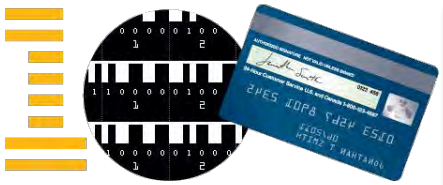
LGPDPPSO Artículo 33 Frac. XXXIII
Lineamientos Generales 59

DS

Riesgo inherente en los sistemas de tratamiento

Paso 4. Inventario de datos personales

Ejemplo de **categorías** de los sistemas de tratamiento, en función del riesgo inherente:



Especial:

Por su naturaleza y contexto pueden causar daño directo a los titulares.

Sensible:

Datos patrimoniales, ubicación física, jurídicos, autenticación, sensibles.

Estándar:

De contacto, identificación, académicos, y laborales.

Manos a la obra

Categorías de los sistemas de tratamiento

Categoría de los sistemas de tratamiento de datos personales	Tipo de datos personal
Estándar	Nombre, teléfono, teléfono celular, correo electrónico, edad, sexo, CURP, RFC, estado civil, experiencia laboral, cédula profesional.
Sensible	Datos de salud: resultado de la audiometría, dirección, número de tarjeta bancaria, historial médico.
Especial	

Ejercicio 2.
Categorías de datos personales en los sistemas de tratamiento

- **Datos Estándar:** Nombre, teléfono, correo electrónico, edad, sexo, CURP, RFC, estado civil, datos laborales.

- **Datos Sensibles:** Estado de salud, ubicación, número de tarjeta bancaria.

¿Qué debe contener un inventario de datos personales?

01	02	03	04	05	06
Catálogo de medios físicos y electrónicos y sus finalidades	Catálogo de los tipos de datos personales que se traten	Catálogo de formatos de almacenamiento	Servidores públicos que tienen acceso a los sistemas de tratamiento	Nombre completo o denominación o RFC del encargado y el instrumento jurídico	Destinatario o terceros receptores de las transferencias

LGPDPPSO Art. 33 Frac. III – Lineamientos Generales Art. 58

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

¿Dudas?

seguridatos@inai.org.mx

Armando Becerra ***@ninjamachete***

Noemi González ***@nkglez***

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

TALLER MEDIDAS DE SEGURIDAD SECTOR PÚBLICO

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES – PARTE 2

SECTOR PÚBLICO 2018

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

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN

Armando Becerra *@CiberArmand*

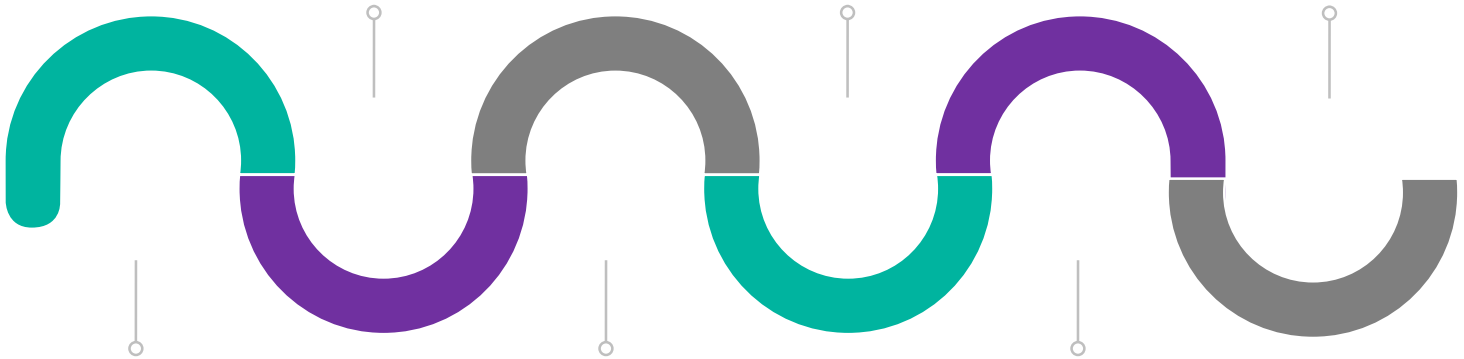
Noemi González *@nkglez*

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

Paso 5. Realizar el 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

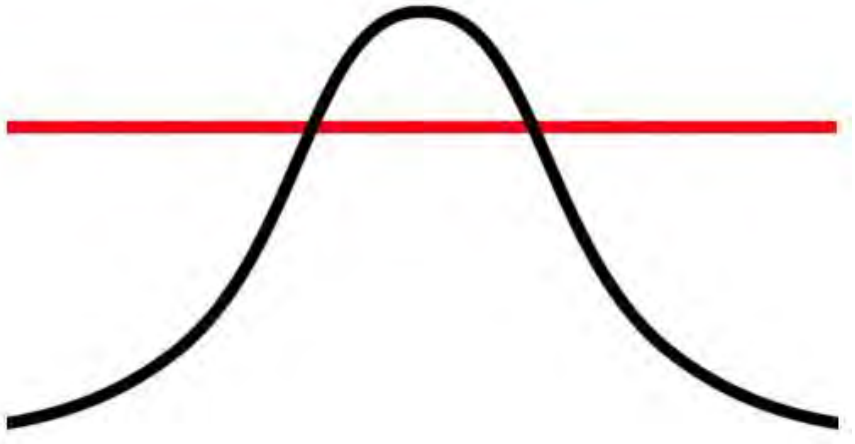
Aceptación

Daño a los titulares

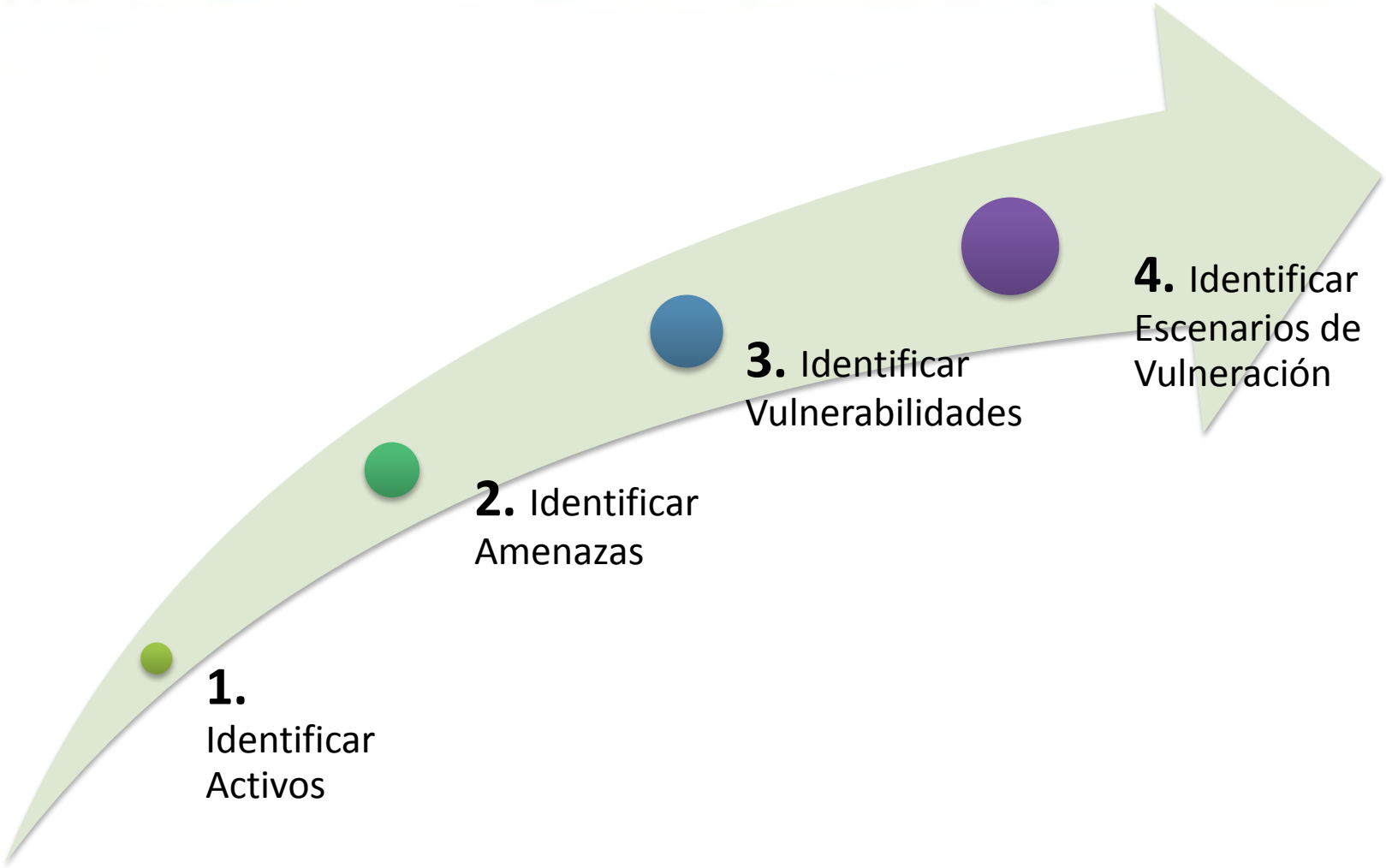
Daño a la organización

Criterios de evaluación del riesgo de IMA

- 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

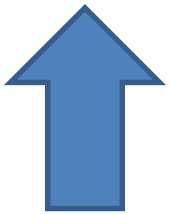


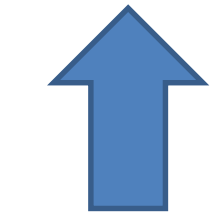
1. Identificar activos

Activos de Información

Activos de Apoyo

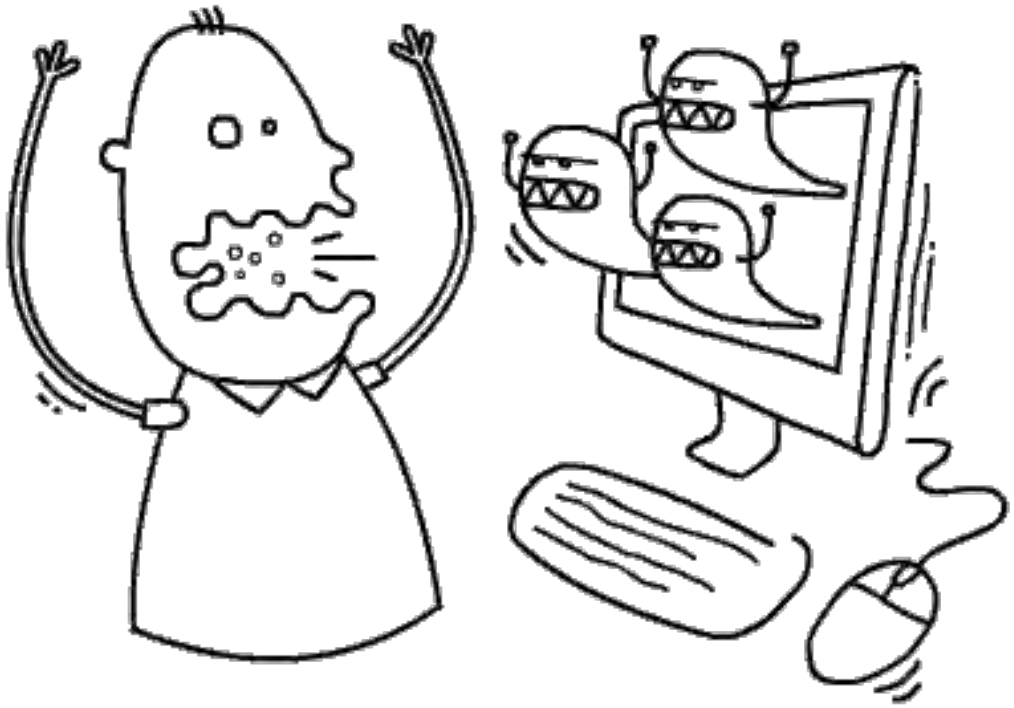
1. Identificación de Activos de IMA





Empleados Prospectos Pacientes

2. Identificar Amenazas



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 del IMA

Fuego

Virus

3. Identificar Vulnerabilidades

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

3. Vulnerabilidades de los Activos del IMA

Material susceptible al fuego

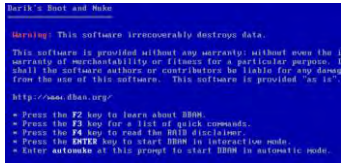
Falta de antivirus

4. Identificar Escenarios de Vulneración

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

4. Escenarios de Vulneración de los Activos del IMA



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





Manos a la obra

Ejercicio 3. Análisis de Riesgos de los Datos Personales

Activo	Amenazas	Vulnerabilidad	Impacto
Expediente de Personal	Tuberías antiguas	Humedad	Daño
Resultado de Audiometría	Falla de suministro eléctrico	Equipo médico susceptible a variación de voltaje	Alteración o modificación
Base de datos prospectos	Empleado descontento	Falta de vigilancia en la entrada	Robo
Computadora	Corrupción de datos	Falta de respaldos	Pérdida

Demo. “Datos Borrados”

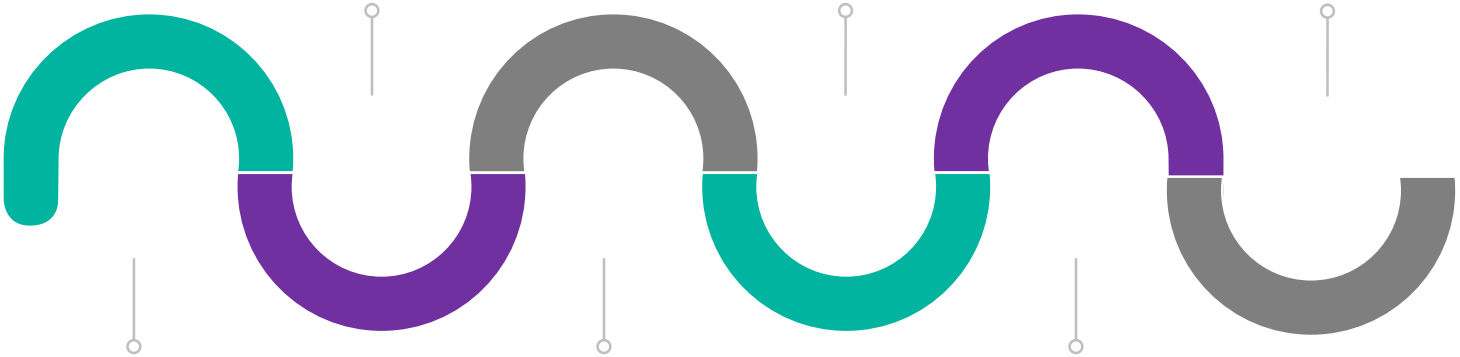
DEMO TIME 

Fase 1

Paso 2. Política de Gestión de DP

Paso 4. Inventario de DP

Paso 6. Análisis de Brecha



Paso 1. Alcances y Objetivos

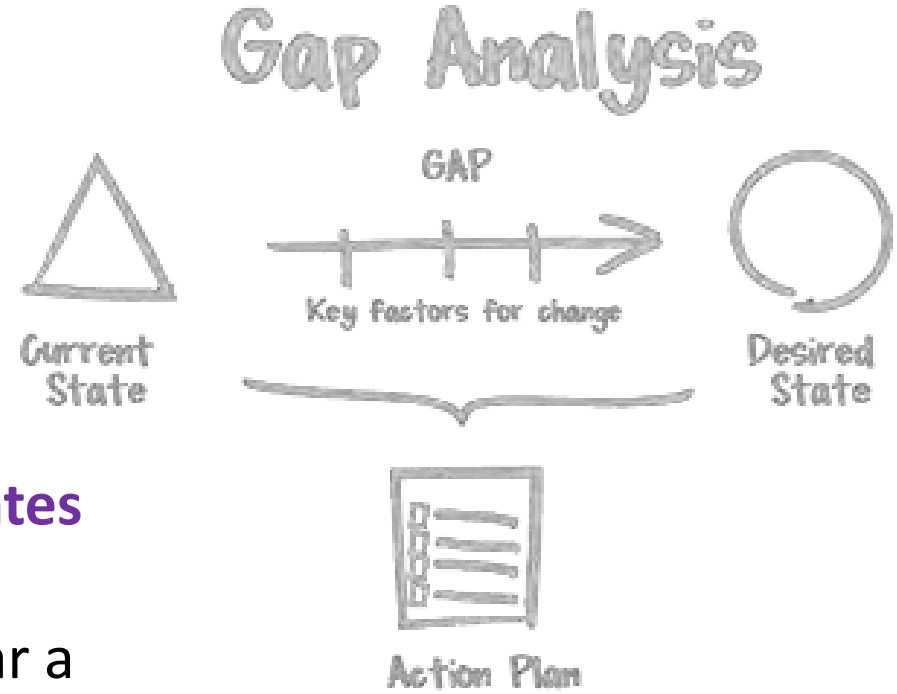
Paso 3. Funciones y Obligaciones

Paso 5. Análisis de Riesgo de DP

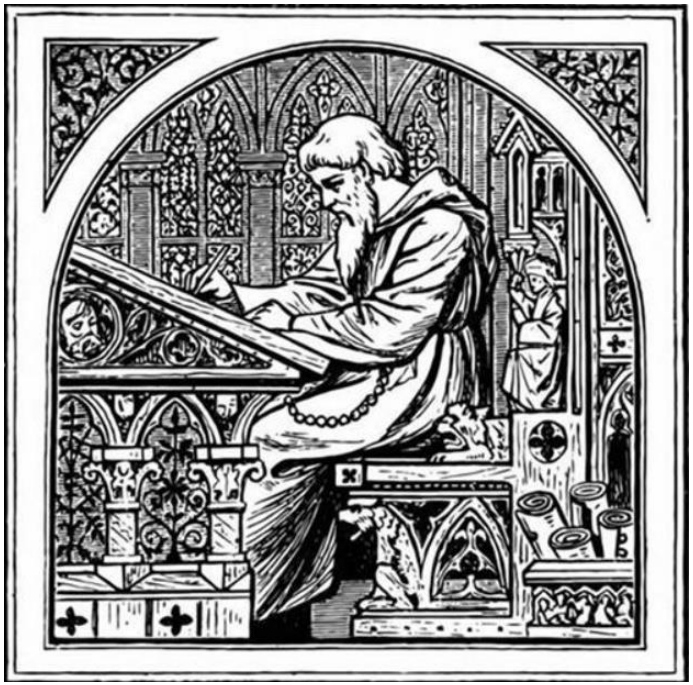
Paso 6. Identificación de las medidas de Seguridad y Análisis de Brecha

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.



Políticas del SGSDP



DS

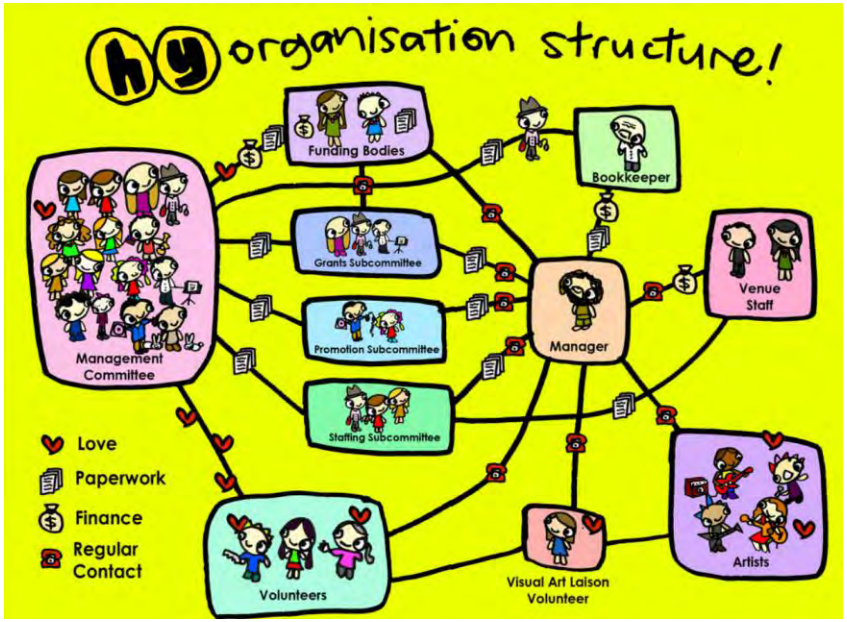
Dominios controles (cont.)

Cumplimiento Legal

DS

Dominios controles (cont.)

Estructura organizacional de la seguridad



DS

Dominios controles (cont.)

Clasificación y acceso de los activos

Dominios controles (cont.)

Seguridad del personal

DS

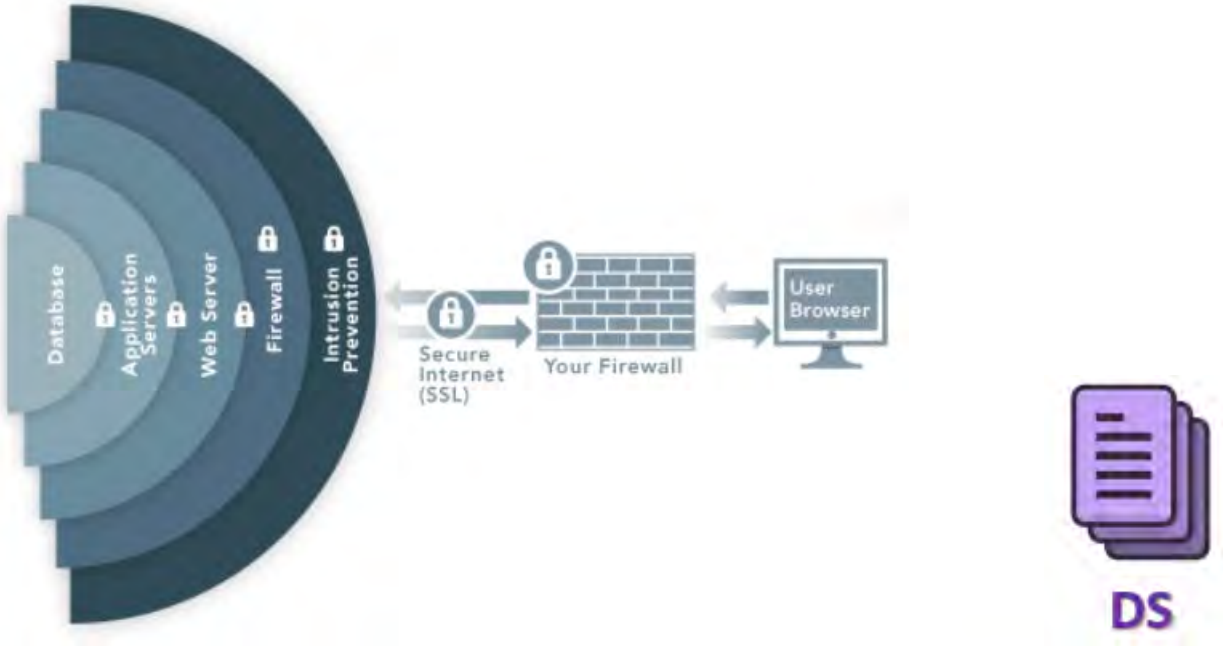
Dominios controles (cont.)

Seguridad física y ambiental

DS

Dominios controles (cont.)

Gestión de comunicaciones y operaciones



Dominios controles (cont.)

Control de acceso

Dominios controles (cont.)

Desarrollo y mantenimiento de sistemas

DS

Dominios controles (cont.)

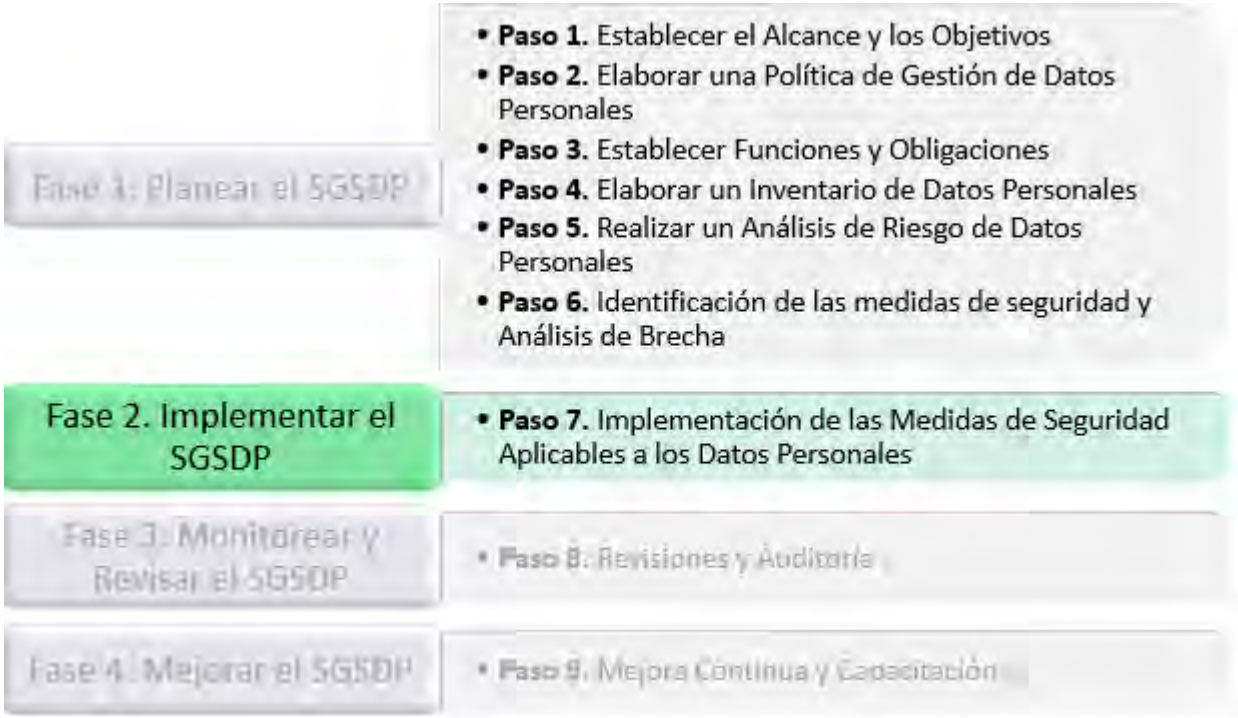
Vulneraciones de seguridad

DS

Análisis de Brecha del IMA

¿Qué dominios de controles ya tiene cubiertos IMA?

¿Qué dominios podrían ayudar a mitigar los escenarios de riesgo identificados?



FASE 2: IMPLEMENTAR EL SGSDP

Cumplimiento Cotidiano de Medidas de Seguridad

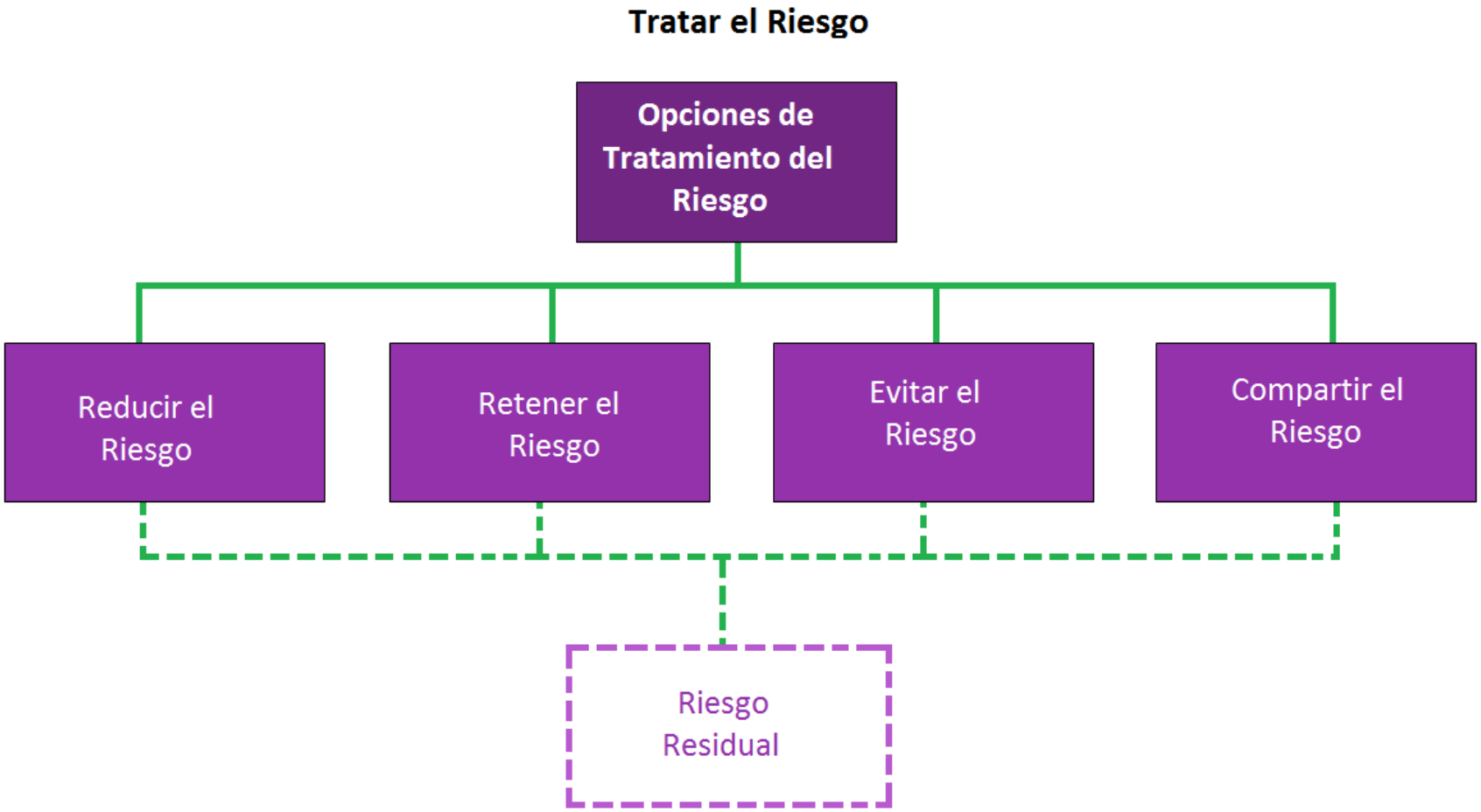
Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes

Cumplimiento Cotidiano de Medidas de Seguridad

Cumplimiento Cotidiano en el IMA

- En seguimiento del compromiso establecido por el Director General, los Subdirectores colaboran para vigilar el cumplimiento día a día, por ejemplo, señalando a los empleados que no portan gafete sobre este hecho.

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

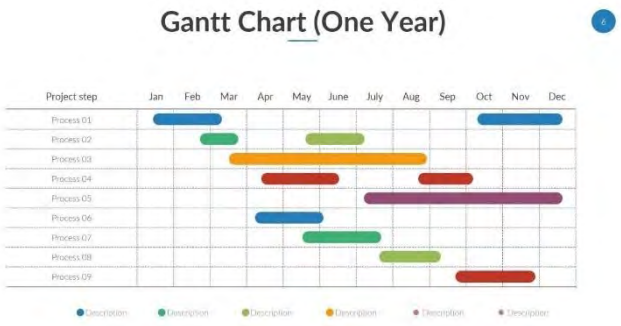
Compartir el Riesgo. Un tercero interviene para mitigar los posibles efectos de un riesgo.

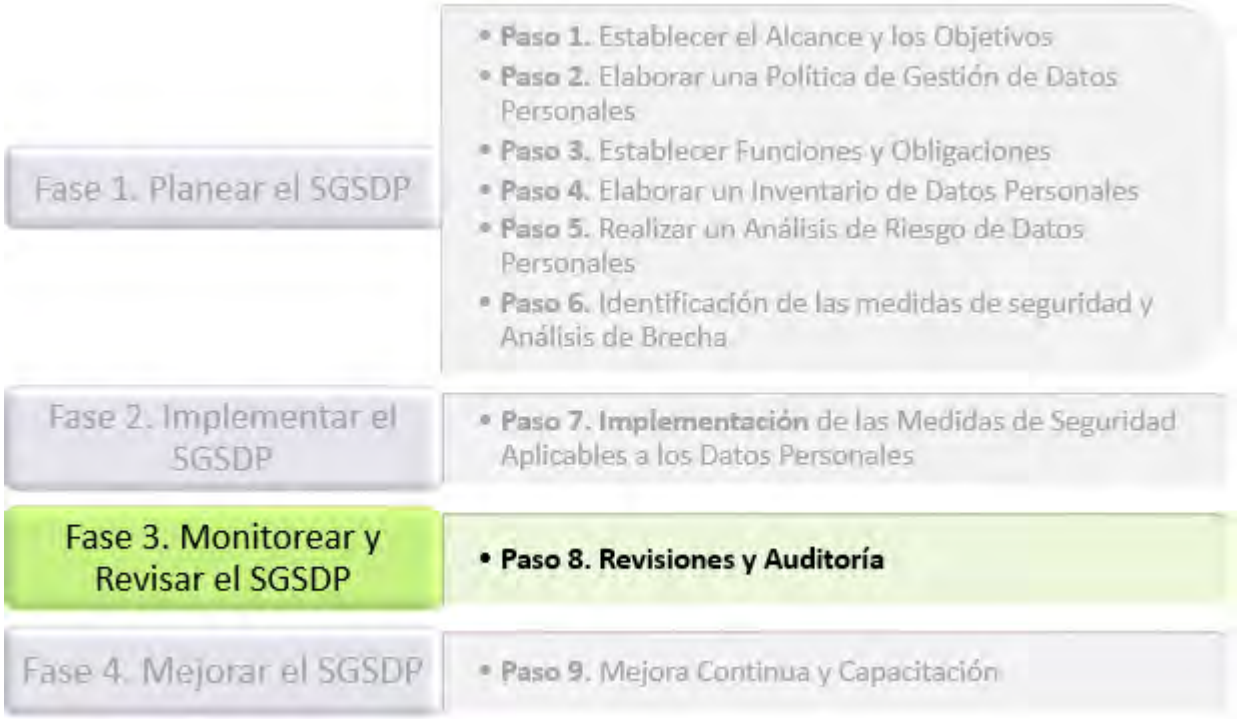
Aceptar

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

Plan de Trabajo de IMA

Reducir	Retener	Evitar	Compartir
• Comprar antivirus • Comprar un regulador de voltaje • Política de respaldos de la información	• Robo de las bases de datos por un servidor público descontento	• Mover los archiveros lejos del baño	• Ninguno





FASE 3: MONITOREAR Y REVISAR EL SGSDP

Paso 8. Revisiones y Auditoría

Revisión de los factores de riesgo

Auditoría

Vulneraciones a la Seguridad de la Información

Vulneraciones a la seguridad

- Robo
- Pérdida
- Acceso
- Daño

Vulneración a la seguridad de IMA

DEMO TIME 

Ejercicio 4. ¿Cuál es el mejor control?

Manos a la obra

Ejercicio 4. Solución

Dominio: Control de acceso

Objetivo de control: Equipos sin atender

Acciones en caso de vulneración a la seguridad

1) Identificación de la vulneración

2) Notificación de la vulneración

3) Remediación del incidente

FASE 4: MEJORAR EL SGSDP

Paso 9. Mejora continúa y capacitación

Acciones correctivas

Acciones preventivas

Capacitación

Concienciación

Entrenamiento

Educación

Después de la vulneración en IMA

- Se han establecido **políticas de bloqueo del equipo** y diferentes privilegios para tener acceso a las bases de datos.
- Para **identificar otros escenarios y prevenir incidentes**, se contratarán servicios de un especialista para que evalúe la seguridad de la empresa.
- De los resultados de la evaluación del especialista se diseñará un **plan de capacitación**.

¿Y que aprendimos hoy del 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

Conclusiones

- ¿Crees que las acciones que llevó el Instituto Mexicano de Audición para implementar el **Sistema de Gestión de Seguridad de Datos Personales** mejoraron los procesos y la cultura de la organización?


9
7

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

¿Dudas?

seguridatos@inai.org.mx

Armando Becerra ***@ninjamachete***

Noemi González ***@nkglez***