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

TALLER: MEDIDAS DE SEGURIDAD

GUÍA PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES 2019

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN

Miriam J. Padilla Espinosa

Subdirectora de Seguridad de Datos Personales del Sector Privado

@Ing_Mili

¡Bienvenido a tu Taller!

Horario del taller: 10:00 a 15:00 pm

Recesos: Un descanso de 15 a 20 minutos, indicado por el instructor

Agenda:

- Principios y obligaciones de la Ley
- Importancia de la seguridad de los datos personales
- Publicaciones en materia de seguridad del INAI
- Definiciones útiles
- Implementación de un SGSDP – Caso Audidatos

Derechos, principios y deberes rectores del derecho de protección de datos personales

- **A**cceso
- **R**ectificación
- **C**ancelación
- **O**posición

DERECHOS

- Licitud
- Lealtad
- Consentimiento
- Información
- Proporcionalidad
- Finalidad
- Calidad
- Responsabilidad

PRINCIPIOS

- **Seguridad**
- Confidencialidad

DEBERES

¿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 afectaciones económicas debido a **multas**.
- Aumenta la **competitividad**.

Sección de Sector Privado- Público

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

Sección de Sector Privado

Guía de esquemas de autorregulación en materia de protección de datos personales

diciembre 2016

http://rea.inai.org.mx/

Publicación de documentos, y otras referencias respecto al deber de seguridad (Cont.)

Documento orientador para la elaboración del Programa de Protección de Datos Personales

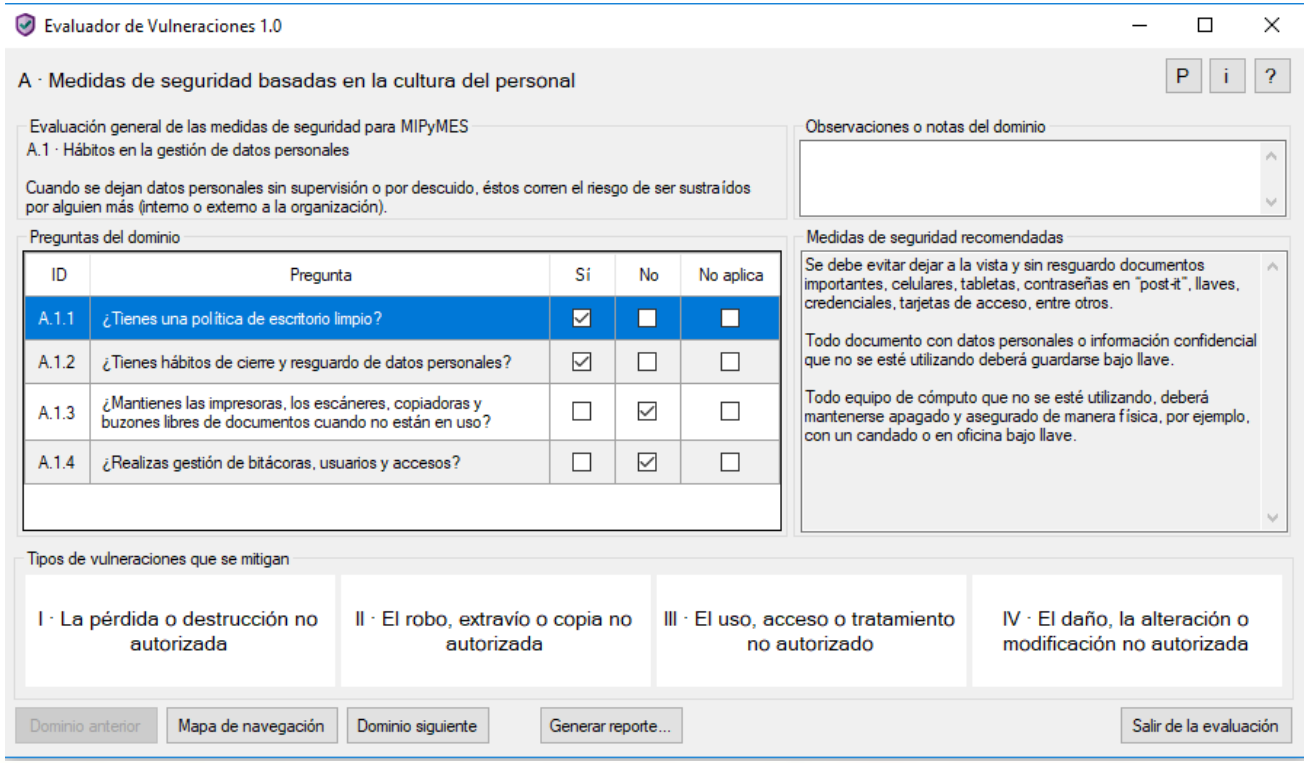
9 agosto 2018

- ANEXO0-EsquemaGeneralPPDP
- ANEXO1-InventariodeTratamientos
- ANEXO2-PrincipiodeInformacion
- ANEXO3-EjAPIntegral
- ANEXO4-EjAPSimplificado
- ANEXO5-AutoevaluacionAP
- ANEXO6-1-Vulneraciones
- ANEXO6-MedidasdeSeguridad
- ANEXO7-DerechosARCO
- ANEXO8-ReglasdeRepresentacion

Anexos del documento orientador para la elaboración del Programa de Protección de Datos Personales

9 agosto 2018

Evaluador de Vulneraciones



Recomendaciones en materia de Seguridad de Datos

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

DEFINICIONES

Definiciones

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**

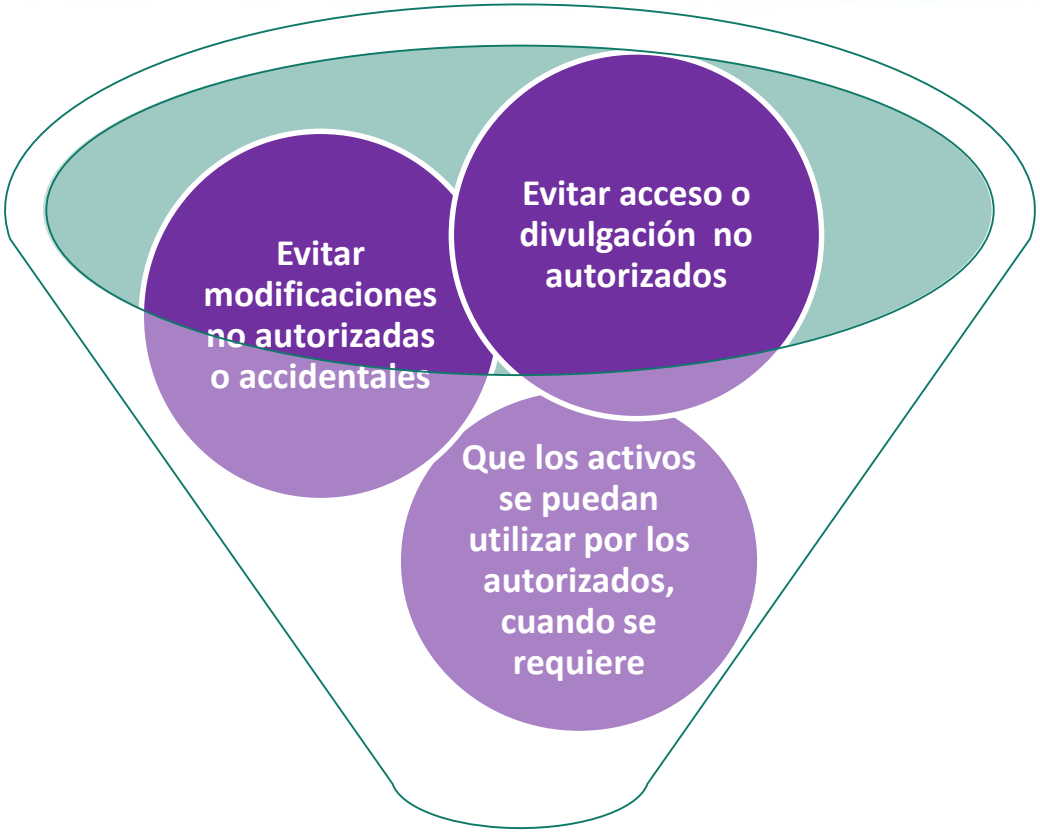
Alta Dirección

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

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

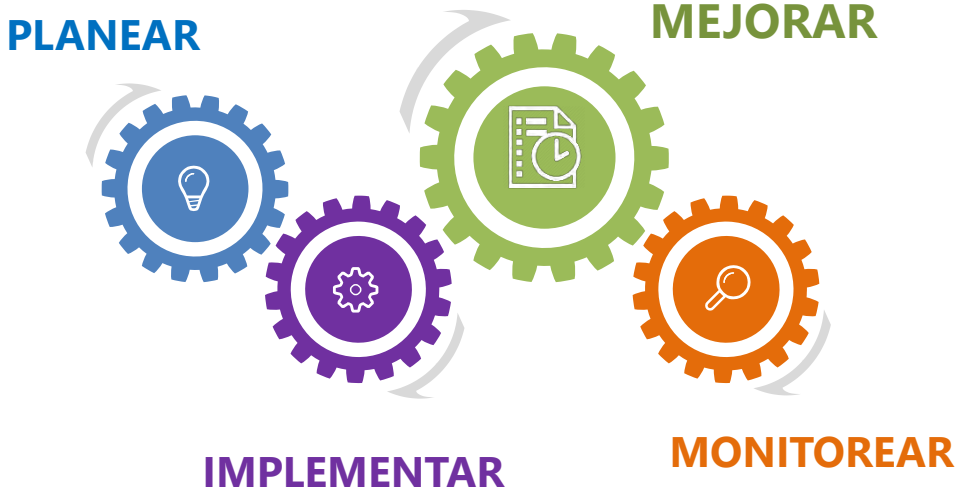
Monitoreo y revisión periódica medidas seguridad

Capacitación basada en niveles

Sistema de Gestión de Datos Personales

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, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.



Sistema de Gestión de Seguridad de Datos Personales

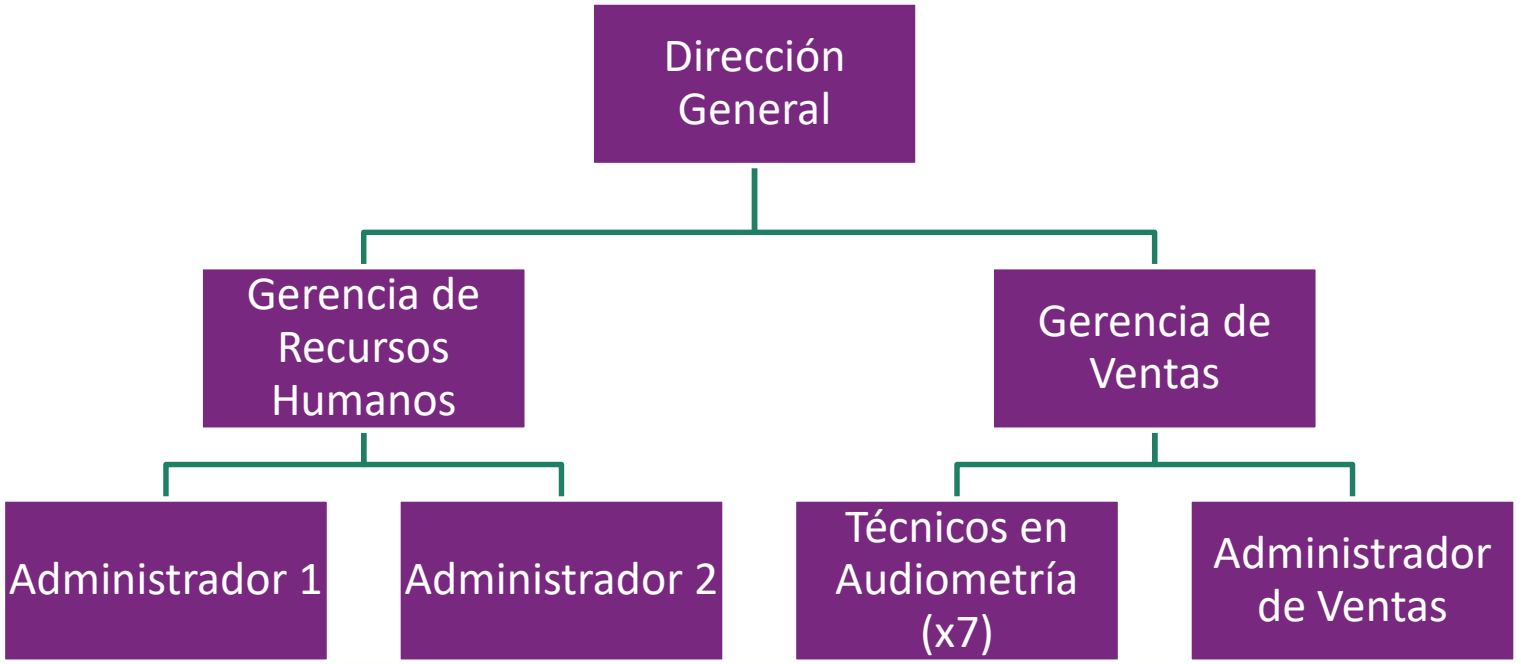
Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** Elaborar un Inventario de Datos Personales • **Paso 5.** Realizar un Análisis de Riesgo de Datos 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

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

Caso de estudio: Audidatos S.A. de C.V.

Caso Audidatos S.A. de C.V

- **AudiDatos** es una empresa dedicada a la venta de equipo médico auditivo que inició sus operaciones en 2005. Con la entrada en vigor de la LFPDPPP en 2010 y posteriormente de su Reglamento en 2011, la empresa ha trabajado para alinear sus prácticas al tratamiento legítimo de los datos personales.



Caso Audidatos S.A. de C.V

- **Organización de la compañía**

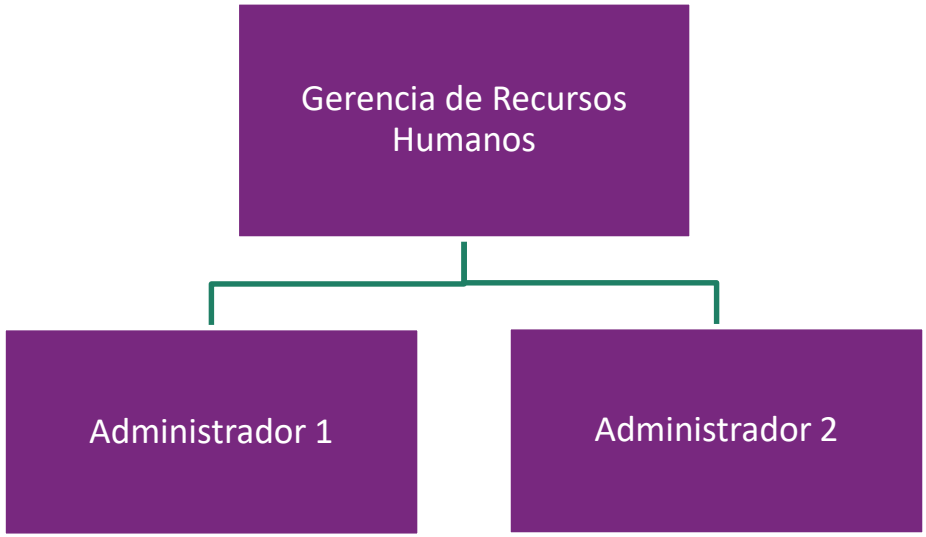
Dirección General

El Director General es el dueño de la empresa y por tanto, responsable ante la Ley. Para este caso de estudio tomaremos en consideración la Gerencia de Recursos Humanos y la Gerencia de Ventas.

- **Gerencia de Recursos Humanos**

El Gerente de Recursos Humanos tiene a cargo dos administradores de tiempo completo, quienes realizan las siguientes actividades:

- **Administración de expedientes del personal**
- **Trámite de solicitudes de los titulares para el ejercicio de los Derechos ARCO**



Caso Audidatos S.A. de C.V

De manera interna el área de **Recursos Humanos** de AudiDatos recaba la información de su personal para generar un ***expediente*** de cada empleado, poniendo a disposición el aviso de privacidad correspondiente y solicitando: datos de contacto, laborales y académicos, de salud y bancarios, tales como: nombre, teléfono, edad, sexo, CURP, estado civil, experiencia laboral, cédula profesional, número de tarjeta bancaria, historial médico, entre otros. Dichos expedientes son almacenados en la **base de datos de Empleados**, la cual se resguarda en un archivero bajo llave, en la oficina. Antes de firmar el contrato laboral, al empleado se le explican las cláusulas correspondientes al desempeño de sus funciones, incluyendo cláusulas de confidencialidad.

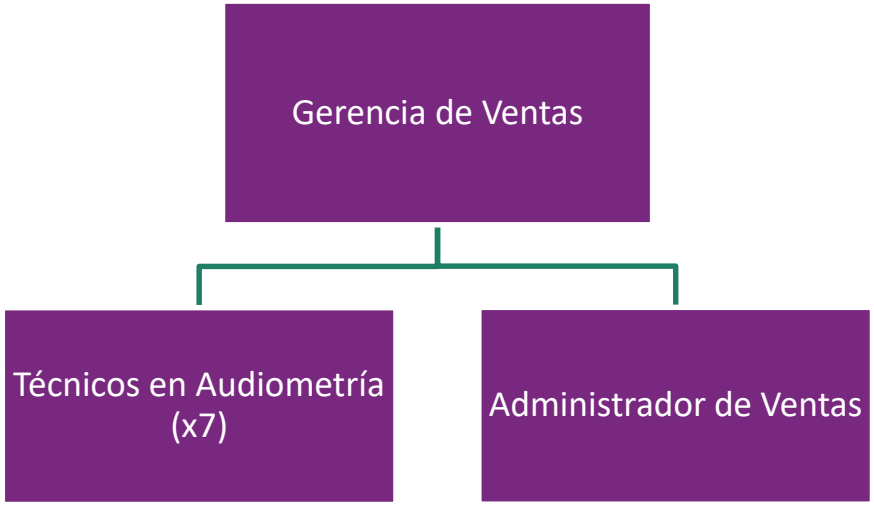
Finalmente, otra de las tareas cotidianas del área es atender las solicitudes de los titulares para el ejercicio de los Derechos ARCO.

Caso Audidatos S.A. de C.V

- ## Gerencia de Ventas

El Gerente de Ventas, es el coordinador de 7 *Técnicos en Audiometría*, los cuales se encargan de:
Realizar la venta de dispositivos
Prospectar clientes

Por su parte el *Administrador de Ventas* se encarga de:
Gestión de prospectos, clientes y proveedores



Caso Audidatos S.A. de C.V

El equipo de **Ventas** está conformado por *Técnicos en Audiometría* los cuales atienden a los pacientes que van a las instalaciones por problemas de sordera. El *Técnico en Audiometría* recibe al paciente y lo atiende de manera personalizada, pone a su disposición el aviso de privacidad y procede a recabar sus datos como nombre, dirección y teléfono en un *formulario de servicio* impreso. El Técnico le explica al paciente que debido a que obtendrán sus datos de salud con el *resultado de la audiometría*, necesitará que le firme el formato para obtener su consentimiento expreso.

Caso Audidatos S.A. de C.V

Una vez que el Técnico en Audiometría obtiene los resultados de la evaluación, le presenta al paciente los distintos modelos de aparatos disponibles, que cubren sus necesidades. Para concluir con la compra, se emite la factura y se le entrega al cliente un formato para evaluar el servicio y responder si desea ser contactado posteriormente y darle seguimiento a su tratamiento. De todos estos formatos recabados se genera un expediente digitalizado por cliente y se almacena en la **base de datos de Clientes** ubicada en la computadora del Gerente de Ventas.

Caso Audidatos S.A. de C.V

En caso de que el paciente decida no realizar la compra en ese momento, la información se mantiene en la **base de datos de Prospectos** durante dos meses, transcurrido el plazo, se destruye la información personal.

Otra de las actividades de los Técnicos es prospectar clientes potenciales que pudieran requerir los servicios de AudiDatos, esto lo hacen a través de visitas a clínicas y hospitales, donde a través de *formularios en papel* recaban datos de contacto (nombre, teléfono y edad) de los interesados. Esta información también se mantiene en la **base de datos Prospectos, para hacer labor de venta** durante un mes, después de ese tiempo se destruyen los formularios.

Caso Audidatos S.A. de C.V

Por su parte, el Administrador de Ventas contrata a una empresa de publicidad llamada **PubliDatos**, con el fin de realizar campañas y eventos de promoción de sus productos para recabar datos de contacto de los asistentes interesados, los cuales se almacenan en la **base de datos Prospectos**.

FASE 1: PLANEAR EL SGSDP

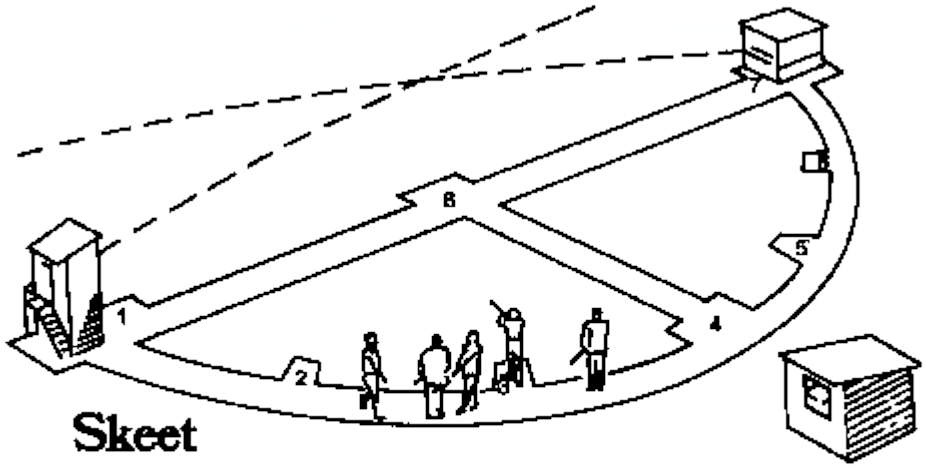
Fase 1

- Paso 1. Alcances y Objetivos
- Paso 2. Política de Gestión de DP
- Paso 3. Funciones y Obligaciones
- Paso 4. Inventario de DP
- Paso 5. Análisis de Riesgo de DP
- Paso 6. Análisis de Brecha

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 Agente de Ventas.

Paciente (Titular)

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

Agente de Ventas (Responsable)

Recibe el resultado de la audiometría.

Entrega el resultado de la audiometría consentida por el paciente.

Manos a la obra

Ejercicio 1: Actores Audidatos

Actores	¿Quiénes son los actores involucrados en AudiDatos?
Titular (es)	
Responsable (s)	
Encargado (s)	
Custodio (s)	
Alta gerencia	

Ejercicio 1: Actores Audidatos

Actores	¿Quiénes son los actores involucrados en AudiDatos?
Titular (es)	Clientes, Prospectos, Empleados
Responsable (s)	AudiDatos/Director General
Encargado (s)	PubliDatos
Custodio (s)	Administrador 1, Administrador 2, Técnicos en Audiometría, Administrador de Ventas
Alta gerencia	Director General, Gerente de Recursos Humanos, Gerente de Ventas

Fase 1

- Paso 1. Alcances y Objetivos
- Paso 2. Política de Gestión de DP
- Paso 3. Funciones y Obligaciones
- Paso 4. Inventario de DP
- Paso 5. Análisis de Riesgo de DP
- Paso 6. Análisis de Brecha

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**
Los Datos Personales	Recabados a través de formularios en papel	Por los técnicos de Audiometría	Para hacer la labor de venta	Deben ser destruidos	Después de un mes




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

Política de Gestión de DP de Audidatos

- El Director General junto con sus Gerentes de Ventas y Recursos Humanos han redactado una Política de Protección de Datos.

- **“Los Datos Personales recabados a través de formularios en papel, por los Técnicos en Audiometría para hacer labor de venta, deberán ser destruidos después de un mes”.**

Paso 2. Elaboración de una Política de Gestión de Datos Personales (cont.)

Fase 1

- Paso 1. Alcances y Objetivos
- Paso 2. Política de Gestión de DP
- Paso 3. Funciones y Obligaciones
- Paso 4. Inventario de DP
- Paso 5. Análisis de Riesgo de DP
- Paso 6. Análisis de Brecha

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

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
- Apoyar en la implementación, adopción y seguimiento de **medidas de seguridad**.
- Definir **responsabilidades** para la protección de los DP
- Identificar requerimientos específicos en materia de **capacitación** 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

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

Funciones y Obligaciones en Audidatos

- Ambos Gerentes comunican a la gente bajo su cargo la Política de Protección de Datos y formalizarán los mecanismos de rendición de cuentas.

Fase 1

Paso 1. Alcances y Objetivos

Paso 2. Política de Gestión de DP

Paso 3. Funciones y Obligaciones

Paso 4. Inventario de DP

Paso 5. Análisis de Riesgo de DP

Paso 6. Análisis de Brecha

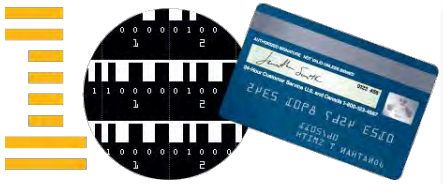
Paso 4. Inventario de datos personales

Ciclo de vida de los Datos Personales

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.

¿Qué puede tener 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	Personal 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

Ejemplo
Inventario de datos personales

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

Unidad administrativa:	Señalar nombre de la unidad administrativa a cargo o administradora del proceso o procedimiento en el que se tratan los datos personales.
Fecha de elaboración o última actualización:	Señalar fecha en la que concluyó la elaboración del inventario o su última actualización
Nombre del tratamiento (proceso):	Señalar nombre del tratamiento.
Fundamento jurídico que habilita el tratamiento:	Señalar las principales
Atribuciones de la unidad administrativa para realizar el tratamiento:	Señalar las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento, entre ellas, las que señala el Reglamento o Estatuto Orgánico interno, y otras si las hul

Medio de obtención de los datos personales (1)			Tercero que transfiere los datos personales, en su caso (2)	Finalidades de la transferencia recibida, en su caso (3)	Listado de datos personales (4)	
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.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del tercero o terceros que realizan la transferencia.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidades se realiza dicha transferencia. Se deberá utilizar la misma fila por tercero que transfiere	Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	En caso de selec opción otro, espe

Manos a la obra

Categorías de los sistemas de tratamiento

Categoría de los sistemas de tratamiento de datos personales	Tipo de datos personal
Estándar	
Sensible	
Especial	

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.

RECESO

Fase 1

- Paso 1. Alcances y Objetivos
- Paso 2. Política de Gestión de DP
- Paso 3. Funciones y Obligaciones
- Paso 4. Inventario de DP
- Paso 5. Análisis de Riesgo de DP
- Paso 6. Análisis de Brecha

Contexto de la Seguridad de Audidatos

AudiDatos cuenta con medidas de seguridad tales como un sistema de control anti-incendios y gafetes, para identificar a todos los empleados, que son revisados por un guardia que trabaja de planta en el edificio. El personal de mantenimiento ha reportado humedad en las paredes del baño contiguo a la oficina donde se almacenan los archiveros con expedientes. Desde que se compró el equipo de cómputo no se han hecho compras de ninguna licencia de software, el equipo de cómputo no está conectado a reguladores de voltaje y aunque los gerentes de vez en cuando copian la base de datos de clientes en dispositivos extraíbles, no cuentan con un procedimiento de respaldos periódicos del contenido del equipo. Todo el personal trabaja con entusiasmo y diligencia, sin embargo, hay rumores de que uno de los Técnicos en Audiometría está molesto con su Gerente.

Paso 5. Realizar el Análisis de Riesgo de los Datos Personales (cont.)

Identificar los sistemas de tratamiento de datos personales

- Conocer los tipos y categorías de datos personales
- Tipos de sistemas de tratamiento –físico o electrónico
- Personal responsable del tratamiento

Definir criterios de aceptación de riesgo y de evaluación

- Riesgo inherente por tipo de dato
- Sensibilidad
- Desarrollo tecnológico
- Posibles consecuencias ante una vulneración
- Número de titulares
- Vulnerabilidades previas
- Requerimientos legales-contractuales
- Valor de los datos personales

Contar con una metodología para la evaluación y tratamiento de riesgos

- Identificar los escenarios de riesgo aplicables
- Amenazas-vulnerabilidades
- Tratamiento del riesgo (mitigar, eliminar, transferir, aceptar)
- Definir las medidas para tratar los riesgos

Paso 5. Realizar el Análisis de Riesgo de los Datos Personales

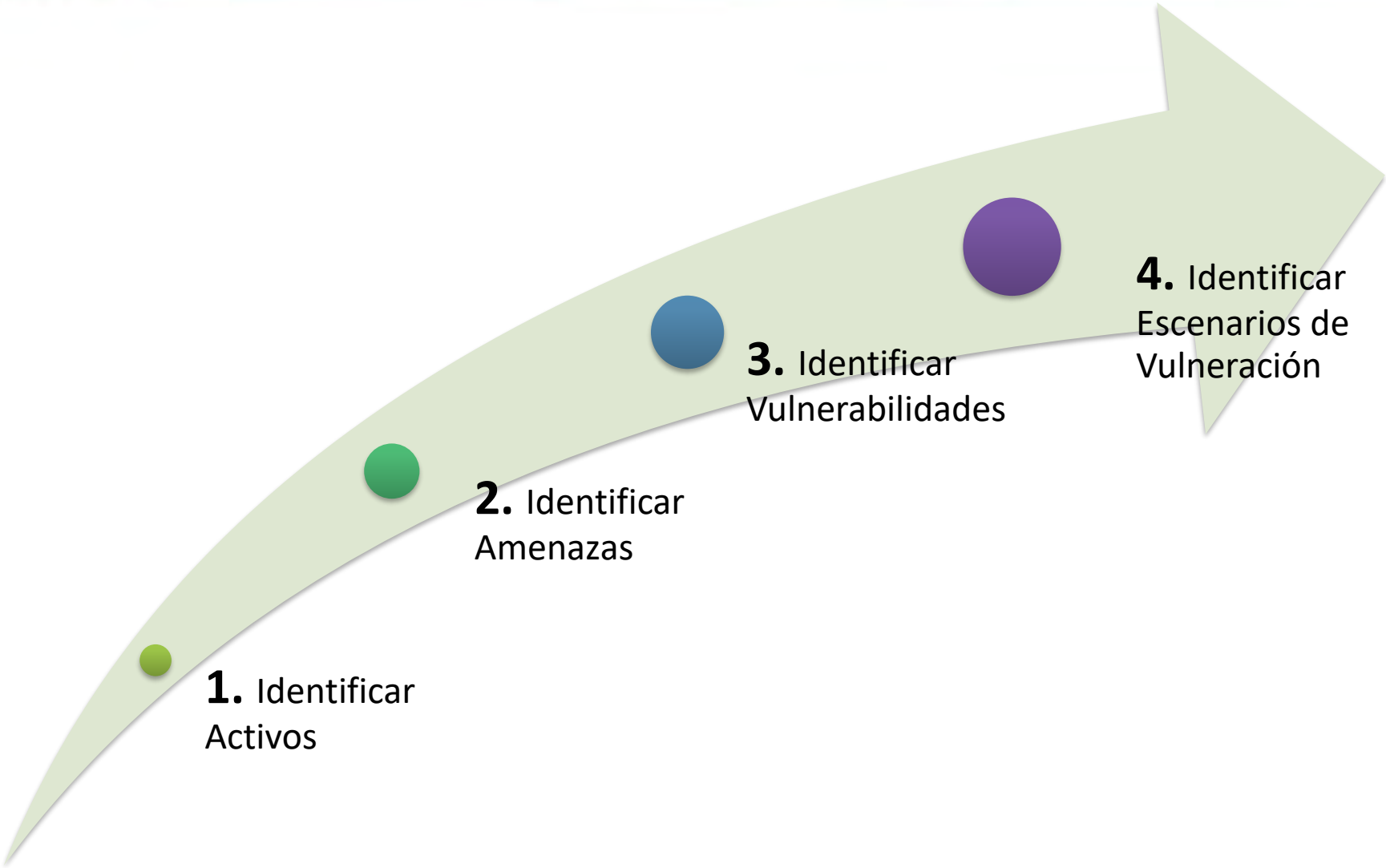
Factores para determinar las medidas de seguridad

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

Paso 5. Realizar el Análisis de Riesgo de los Datos Personales

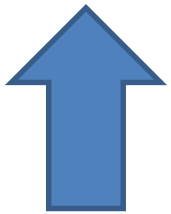


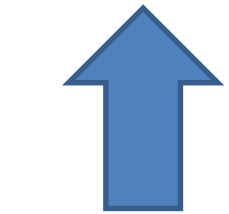
1. Identificar activos

Activos de Información

Activos de Apoyo

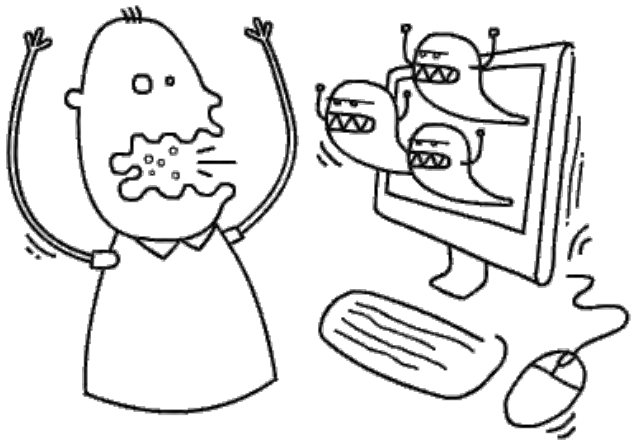
1. Identificación de Activos de Audidatos





Empleados Prospectos Clientes

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 Audidatos

Fuego

Virus

3. Identificar Vulnerabilidades

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

3. Vulnerabilidades de los Activos de Audidatos

Material susceptible al fuego

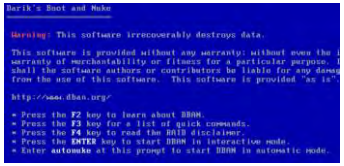
Falta de antivirus

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 de Audidatos



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

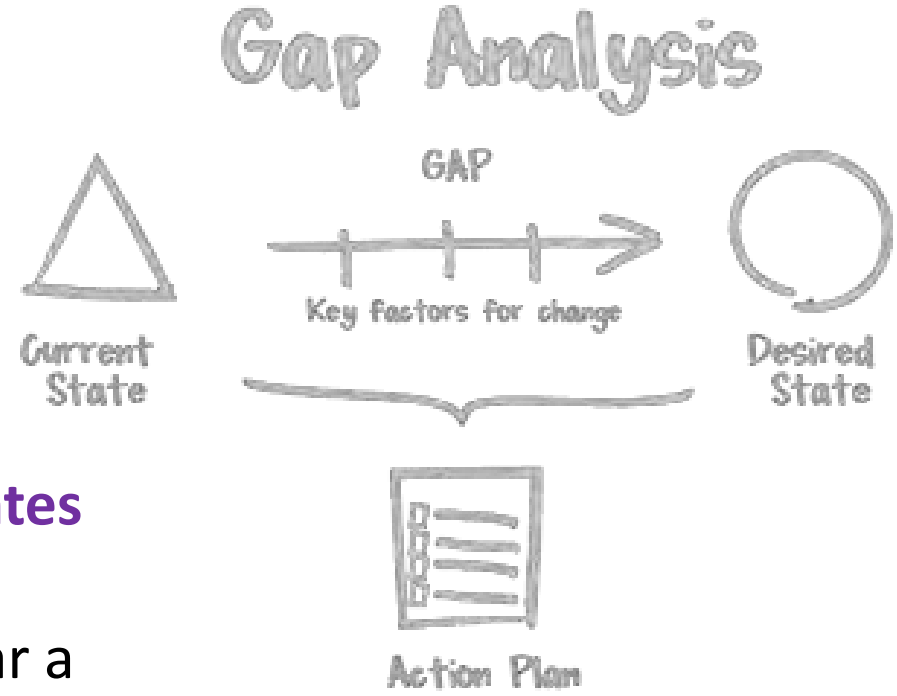
Fase 1

- Paso 1. Alcances y Objetivos
- Paso 2. Política de Gestión de DP
- Paso 3. Funciones y Obligaciones
- Paso 4. Inventario de DP
- Paso 5. Análisis de Riesgo de DP
- Paso 6. Análisis de Brecha

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

El **análisis de brecha** consiste en identificar:

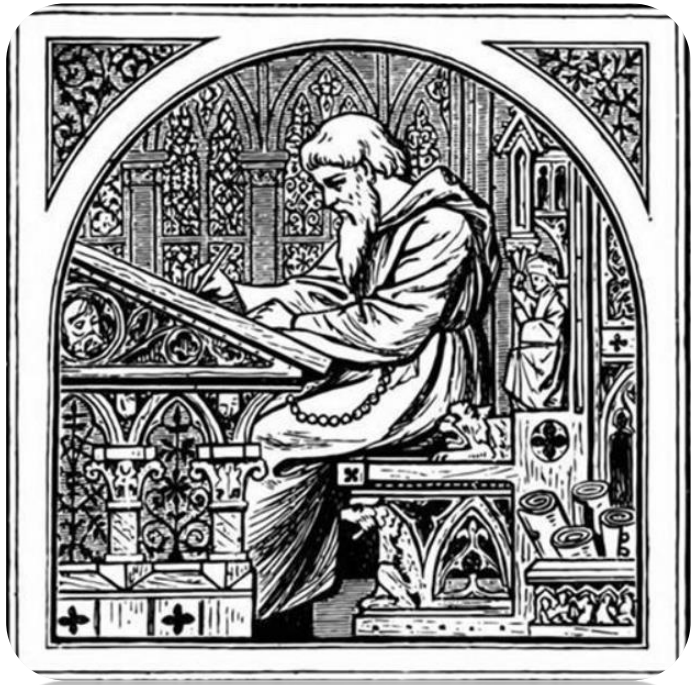
- Las medidas de seguridad **existentes**
- Las medidas de seguridad existentes que **operan correctamente**
- Las medidas de seguridad **faltantes**
- Si existen **nuevas medidas de seguridad** que puedan remplazar a uno o más controles implementados actualmente.



Art 61 LFPDPPP frac. V

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

Políticas del SGSDP

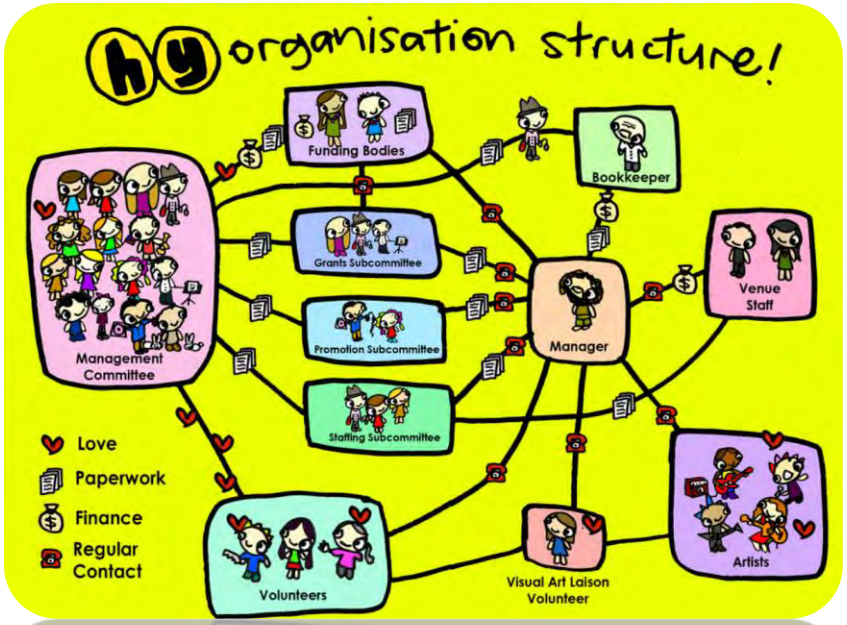


Dominios controles (cont.)

Cumplimiento Legal

Dominios controles (cont.)

Estructura organizacional de la seguridad



Dominios controles (cont.)

Clasificación y acceso de los activos

Dominios controles (cont.)

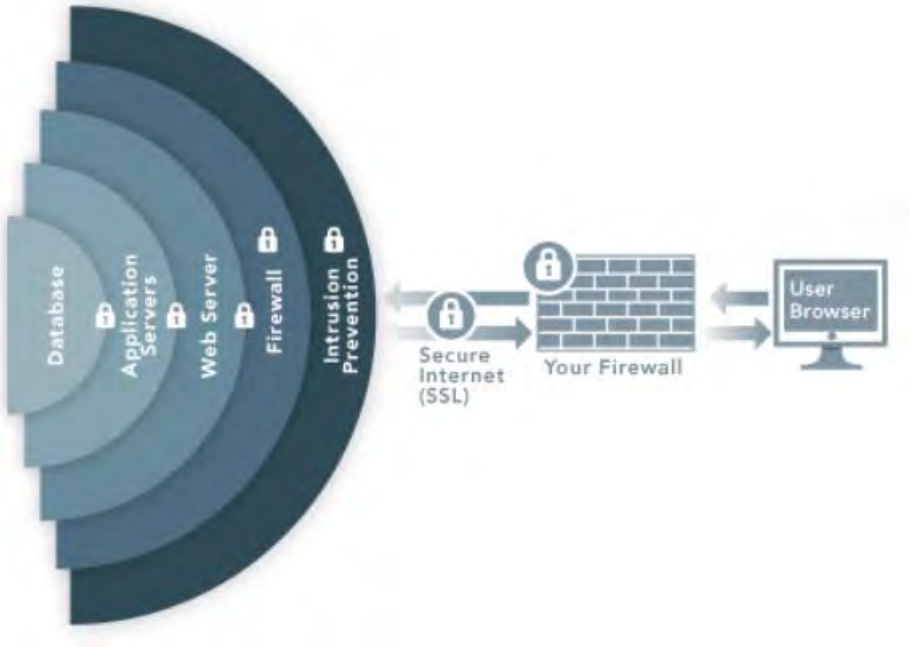
Seguridad del personal

Dominios controles (cont.)

Seguridad física y ambiental

Dominios controles (cont.)

Gestión de comunicaciones y operaciones



Dominios controles (cont.)

Control de acceso

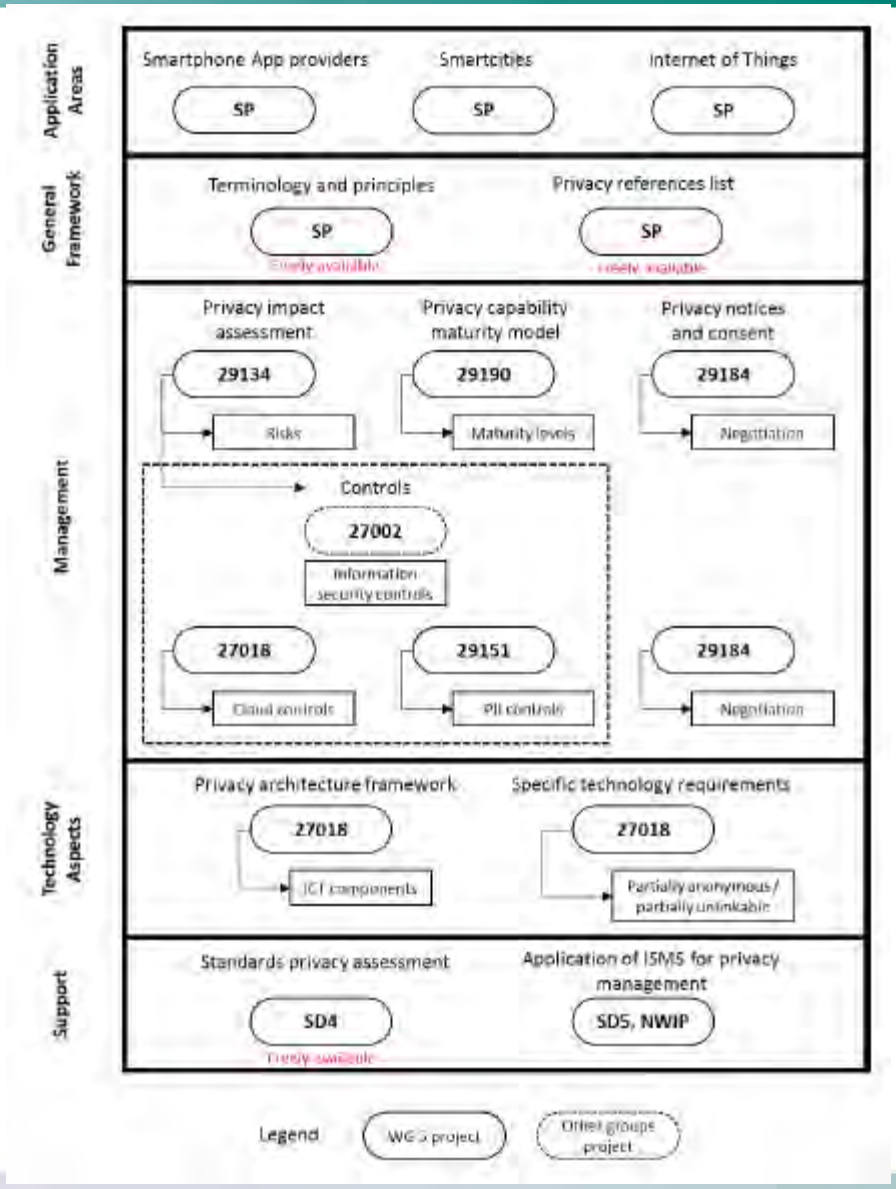
Dominios controles (cont.)

Desarrollo y mantenimiento de sistemas

Dominios controles (cont.)

Vulneraciones de seguridad

Estándares en materia de privacidad y seguridad



ENISA 2019, Guidance and gaps analysis for European standardisation

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

Descripción del control

Evidencia del cumplimiento del control

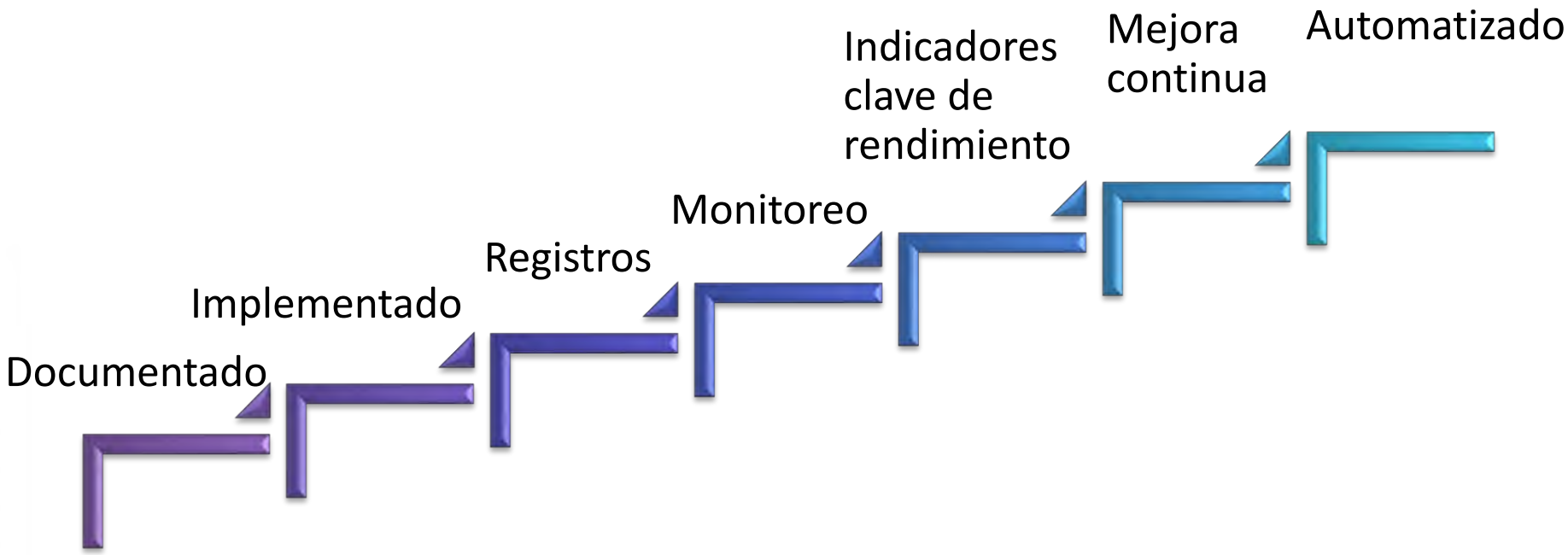
Responsabilidades sobre el control
RACI

POLÍTICAS DEL SGSDP						
CLAVE	CONTROL	DESCRIPCIÓN	EVIDENCIA CUMPLIMIENTO	RACI		
				Responsable	Aprobador	Consultado
PO-01	Políticas de gestión de datos personales	Deben existir políticas aprobadas por la Alta Dirección para la regulación específica, condiciones contractuales, así como para la creación, implementación y mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales y sus activos relacionados durante el tratamiento, que sirvan como guía organizacional del propósito, objetivos, responsabilidades y compromisos establecidos por los involucrados para el cumplimiento de la normatividad aplicable a los datos personales.				
PO-02	Revisión y evaluación	Las políticas relacionadas con el SGSDP deben ser revisadas y evaluadas en su efectividad y cumplimiento periódicamente, así como cuando surja un nuevo riesgo o cambio significativo en la organización				
PO-03	Documentación del SGSDP	Se deben identificar y documentar de manera proporcional a la organización los activos, políticas, acuerdos, planes estratégicos, procedimientos, controles de seguridad, y todo proceso relacionado al				

Facilita identificar las **medidas de seguridad** implementadas y las **responsabilidades** asociadas a la implementación.

Madurez controles

La madurez de los controles puede ser identificada en uno de los siguientes niveles:



Análisis de Brecha de Audidatos

- ¿Qué dominios de controles ya tiene cubiertos Audidatos?
- ¿Qué dominios podrían ayudar a mitigar los escenarios de riesgo identificados?

FASE 2: IMPLEMENTAR EL SGSDP

Implementar y Operar el SGSDP

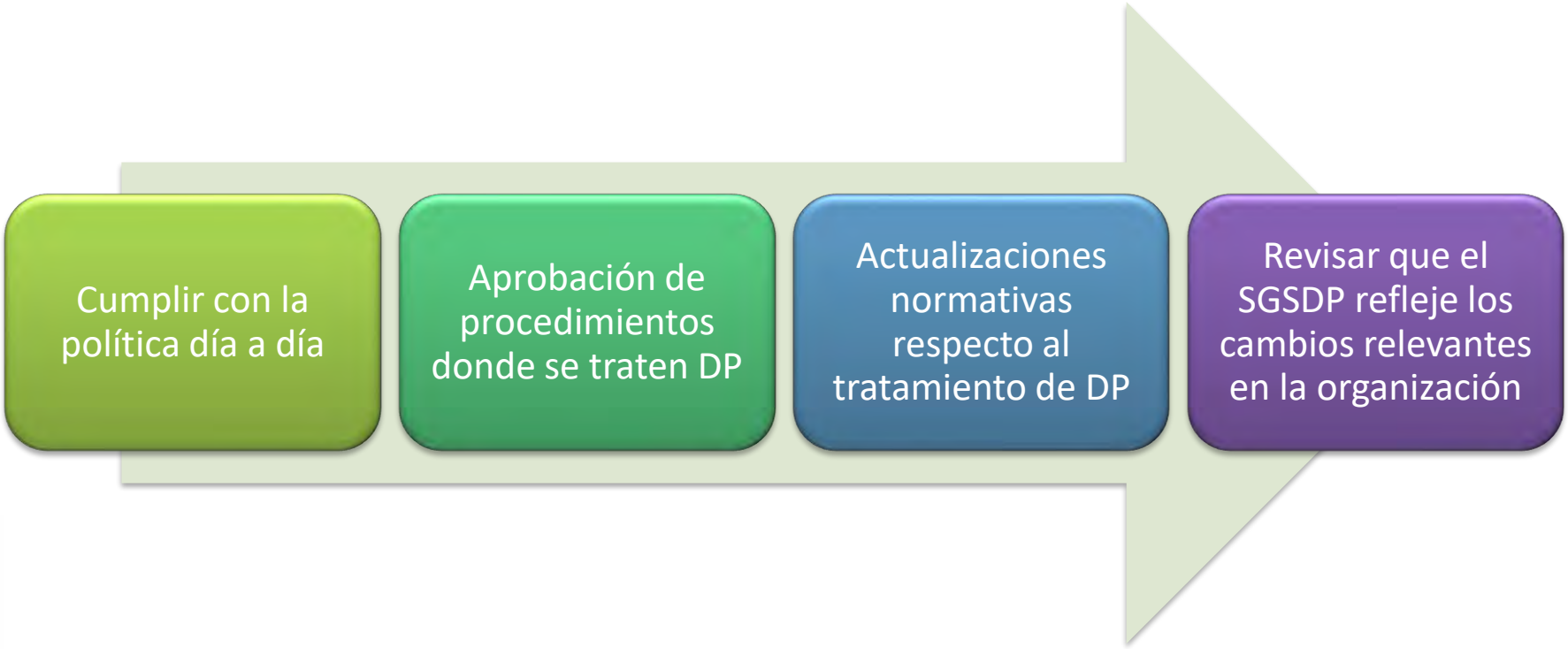
Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales

Paso 7. 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

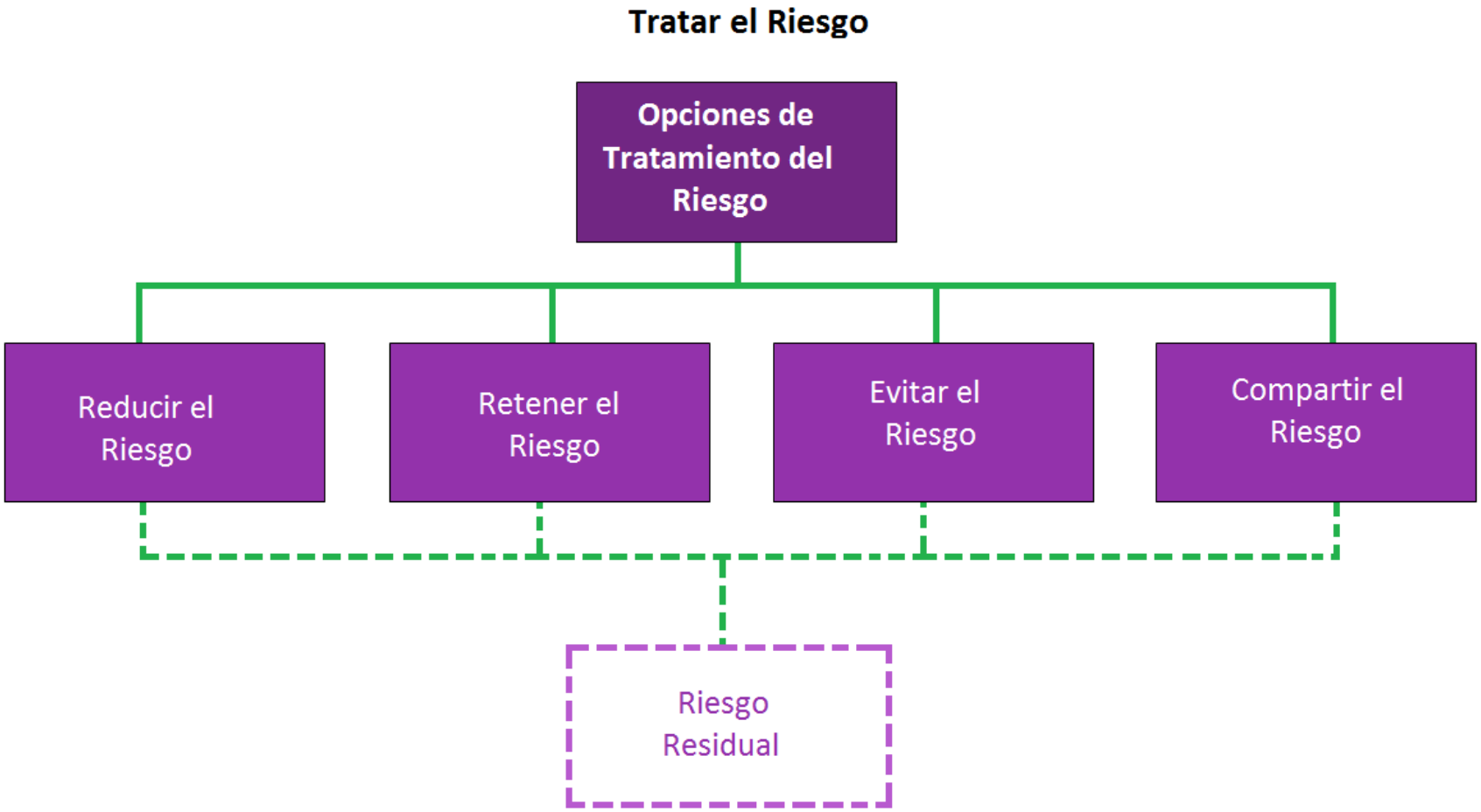
Cumplimiento Cotidiano de Medidas de Seguridad



Cumplimiento Cotidiano en Audidatos

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

Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales



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

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

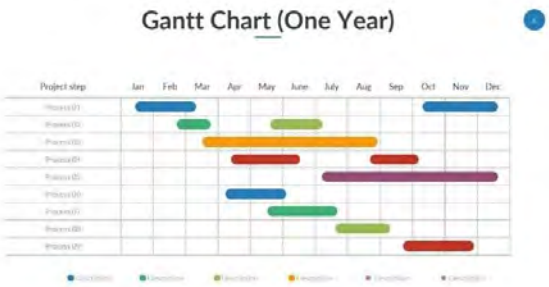
- **Evitar el Riesgo.** Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios.

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

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

Plan de Trabajo de Audidatos

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

Monitorear y Revisar el SGSDP

Paso 8. Revisiones y Auditoría

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 Audidatos

VIDEO TIME

Manos a la obra

Ejercicio 4. Solución

Dominio: Gestión de comunicaciones y operaciones

Objetivo de control: Gestión de soportes informáticos extraíbles

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

Mejorar el SGSDP

Paso 9. Mejora continua y Capacitación

Paso 9. Mejora continúa y capacitación

Acciones correctivas

Acciones preventivas

Capacitación

Concienciación

Entrenamiento

Educación

Después de la vulneración en Audidatos

- Se han establecido **políticas de bloqueo de dispositivos USB** 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 AudiDatos para implementar el Sistema de Gestión de Seguridad de Datos Personales mejoraron los procesos y la cultura de la empresa?

¡Vámonos!

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

GRACIAS

MBA. Miriam Josefina Padilla Espinosa

Subdirectora de Seguridad de Datos Personales del Sector Privado

miriam.padilla@inai.org.mx

@Ing_Mili