Caso de Estudio: Instituto Mexicano de Audición (IMA)

Introducción

El Instituto Mexicano de Audición es una institución dedicada a la ofrecer servicios preventivos y correctivos en pro de una salud auditiva para la población, así como ofrecer la donación de aparatos auditivos a personas de escasos recursos, inició sus operaciones en 2010. Con la entrada en vigor de la LGPDPPSO en 2017 y posteriormente de los Lineamientos Generales, el instituto se encuentra trabajando para alinear sus prácticas al tratamiento legítimo de los datos personales.

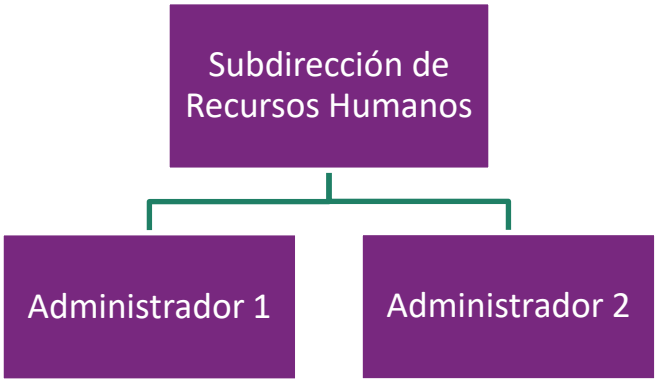
Estructura orgánica

Dirección General

El Director General es la figura de mayor jerarquía en el Instituto.

Para este caso de estudio tomaremos en consideración la Subdirección de Recursos Humanos y la Subdirección de Donaciones.

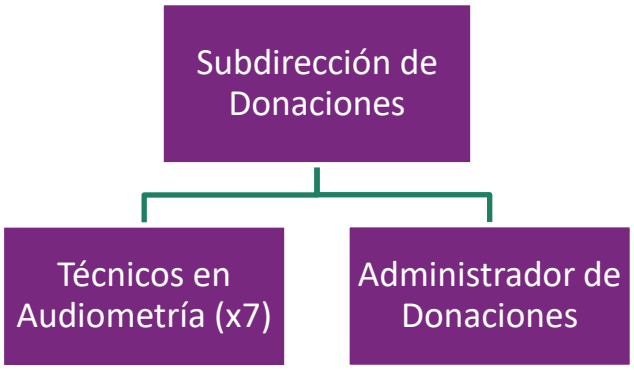
Subdirección de Recursos Humanos



El Subdirector 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**

Subdirección de Donaciones



El Subdirector de Donaciones, es el coordinador de 7 *Técnicos en Audiometría*, los cuales se encargan de:

- **Realizar la evaluación, asignación y entrega de dispositivos a los beneficiados con la donación**
- **Prospectar pacientes que requieran aparatos auditivos**

Por su parte el *Administrador de Donaciones* se encarga de:

- **Gestión de prospectos, beneficiados y proveedores**

Descripción de Procesos

Proceso de Donaciones

El equipo de Donaciones 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, domicilio particular 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.

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 asignación se emite una constancia para avalar el beneficio otorgado 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 paciente y se almacena en la **base de datos de Beneficiados** ubicada en la computadora del Subdirector de Donaciones.

En caso de que el paciente decida no canjear el beneficio 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 pacientes que puedan requerir los servicios del Instituto, 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 prospección en búsqueda de beneficiados** durante un mes, después de ese tiempo se destruyen los formularios.

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

Proceso de Recursos Humanos

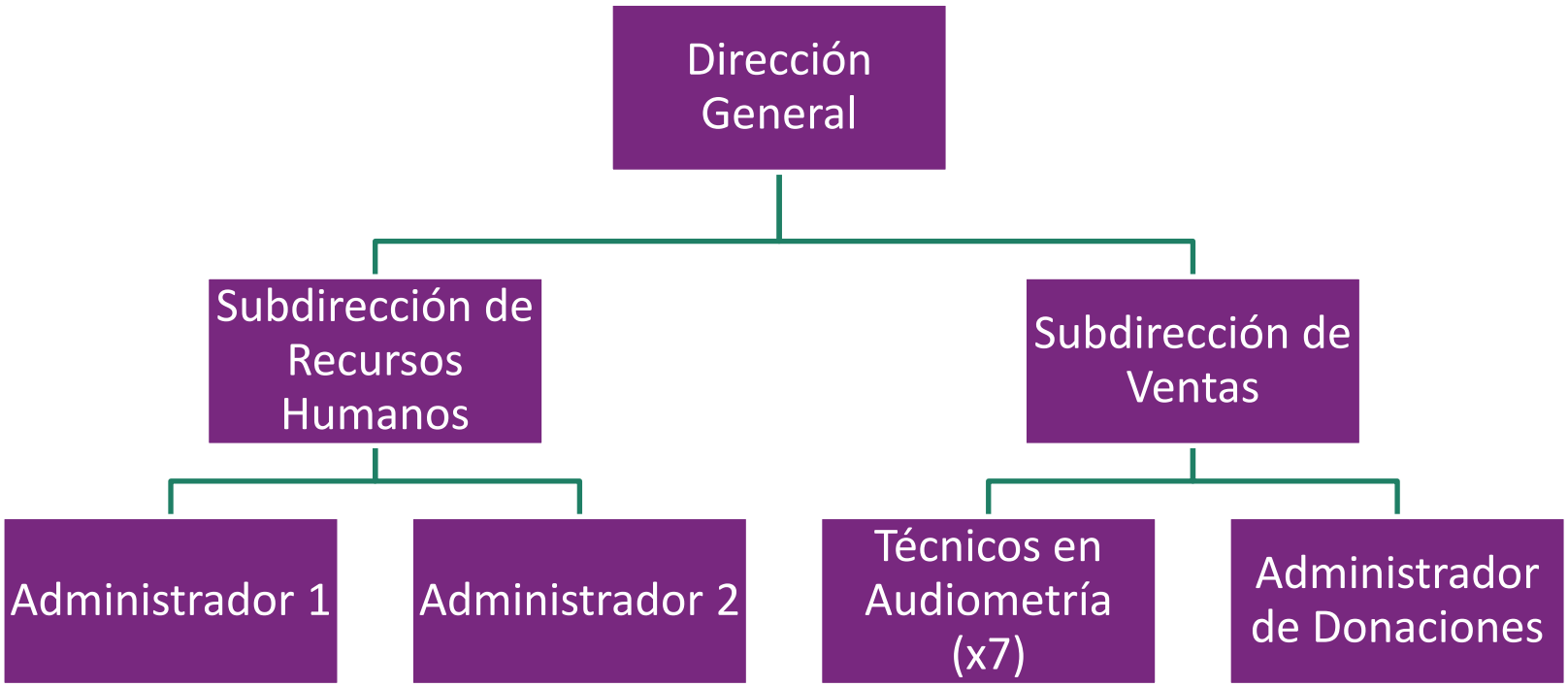
De manera interna el área de Recursos Humanos del instituto recaba la información de su personal para generar un **expediente** de cada empleado, poniendo a disposición el aviso de privacidad correspondiente y solicitando: datos de contacto, laborales y académicos, de salud y bancarios, tales como: nombre, 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.

Contexto de la Seguridad en el Instituto Mexicano de Audición

El Instituto 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 subdirectores 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 Subdirector.

Estructura orgánica del Instituto Mexicano de Audición



Ejercicio 1. Factores contractuales del IMA

Parte 1. Actores que intervienen en las relaciones contractuales

(15 minutos)

Completar la tabla siguiente identificando quiénes son los actores que intervienen en el tratamiento de datos personales, de acuerdo al Caso de Estudio: Instituto Mexicano de Audición

Figura en el tratamiento de datos personales	Actor en el caso de estudio
Titular (es)	
Responsable (s)	
Encargado (s)	
Custodio (s)	
Alta gerencia	

Parte 2. Sigue la pista a los datos personales

(15 minutos)

Una vez identificados los actores en la Parte 1, realiza un diagrama de flujo de cada una de las relaciones contractuales establecidas entre ellos, para los procesos del Caso de Estudio: Instituto Mexicano de Audición.

Proceso de Donaciones	Proceso de Recursos Humanos

Ejercicio 2. Inventario de datos personales

Parte 1. Categorías de datos personales en los sistemas de tratamiento

(10 minutos)

Identificar qué tipo de datos personales son recabados por el Instituto Mexicano de Audición y a qué categoría de los sistemas de tratamiento pertenece, en función de su nivel de riesgo inherente:

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

Parte 2. Aplicación: *Protección INAI*

(15 minutos)

Descargar la aplicación para dispositivos móviles ***Protección INAI*** utilizando el código QR o la liga de descarga a continuación, y realizar el cálculo del riesgo inherente en los sistemas de tratamiento del Instituto Mexicano de Audición.

bit.ly/AppProteccionINAI

Ejercicio 3. Análisis de Riesgo de los Datos Personales

(20 minutos)

De la lista proporcionada, identifica y ordena los **Activos, Amenazas y Vulnerabilidades,** para crear un escenario de riesgo.

- Expediente de personal
- Resultado de audiometría
- Falla de suministro eléctrico
- Tuberías antiguas
- Base de datos de prospectos
- Empleado descontento
- Computadora
- Equipo médico susceptible a variación de voltaje
- Falta de vigilancia en la entrada
- Falta de respaldos
- Corrupción de datos
- Humedad

Ejemplo:

Activo	Amenazas	Vulnerabilidad	Impacto
Expedientes en papel	Incendio	Material susceptible al fuego	Pérdida definitiva de información

Escenario: El **activo** expedientes en papel es susceptibles a la **amenaza** de incendio debido a que tiene la **vulnerabilidad** de ser un material susceptible al fuego, lo que podría tener por **impacto** la pérdida definitiva de la información

Activo	Amenazas	Vulnerabilidad	Impacto
			Daño
			Alteración o modificación
			Robo
			Pérdida

Ejercicio 4. ¿Qué control es el mejor?

(15 minutos)

De los controles siguientes, elige cuál es el mejor control para mitigar el escenario de riesgo mostrado en el ***Demo Time***.

Opción 1. Dominio: Cumplimiento legal

Prevención del mal uso de activos: Se deben tener mecanismos contra el uso de activos para propósitos no autorizados, por ejemplo, para sistemas electrónicos, utilizar bloqueos en caso de que usuarios no autorizados traten de acceder a módulos que no tienen permisos e informar mediante un mensaje el uso indebido.

Opción 2. Dominio: Control de acceso

Equipos sin atender: Los usuarios y contrataciones externas deben tener conocimiento de las medidas de seguridad necesarias para cualquier dispositivo de procesamiento sin atender, por ejemplo, cerrar la sesión cuando se ha terminado de trabajar en la computadora, bloquear el equipo automáticamente cuando no se usa por largos periodos de tiempo, etc.

Opción 3. Dominio: Seguridad del personal

Identificar responsabilidades de seguridad en cada puesto de trabajo : Establecer y dar a conocer a cada, función, rol o puesto las responsabilidades que corresponden respecto a la seguridad y protección de datos personales, informando en su caso de las sanciones de incumplimiento de la política de seguridad.

Opción 4. Dominio: Gestión de comunicaciones y operaciones

Protección contra software malicioso: Deben existir diferentes controles respecto al software malicioso: Prohibir el uso de software ilegal y/o no autorizado. Aplicar difusión (campañas, boletines) sencillos para advertir del software malicioso. Mantener en los dispositivos de procesamiento de información como computadoras, las respectivas herramientas actualizadas que las protejan contra software malicioso. En su caso, monitorear el tráfico y las actividades de red para descubrir cualquier comportamiento anómalo, tales como virus, descargas de contenido inapropiado, fugas de información, etc.