Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas

Junio 2015

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

Contenido

Notas de versiones

- Versión Junio 2015. Respecto a la versión anterior (Julio 2014), se actualizó el nombre, logotipo y sigla del Instituto, debido al cambio de naturaleza jurídica del antes Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), por el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

1. ¿Qué es este documento?

El presente ***Manual en materia de Seguridad de Datos Personales para MIPYMES y organizaciones pequeñas*** (Manual) tiene por objeto orientar a las micro, pequeñas y medianas empresas (MIPYMES), así como a las organizaciones pequeñas, en el cumplimiento de las disposiciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley) y su Reglamento, con relación a las medidas de seguridad para la protección de los datos personales, y para poder implementar el sistema de gestión que sugieren las Recomendaciones en materia de Seguridad de Datos Personales (Recomendaciones), publicadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto) en el Diario Oficial de la Federación (DOF), el 30 de octubre de 2013.

El Manual es un documento que ayuda a los involucrados en el tratamiento de datos personales, en especial a aquellos grupos que están menos familiarizados con el tema de seguridad, a implementar controles de seguridad sencillos, basados en las mejores prácticas y estándares.

2. ¿A quién le interesa este Manual?

☑ A las personas físicas y morales constituidas como MIPYMES u organizaciones pequeñas que realicen tratamiento de datos personales, pues la Ley les exige contar con medidas de seguridad para los datos personales que están en su posesión.

Importante: Público objetivo del Manual

El Manual está dirigido a **los lectores que**:

- **Usan datos personales de: clientes, proveedores, alumnos, usuarios, miembros, empleados, entre otros; para diversas finalidades.**
- **Tienen pocas nociones sobre el tema de protección de datos personales y sobre el tema de seguridad de la información.**

Aquéllos con mayor madurez en el tema de seguridad de la información pueden encontrar documentación más acorde a su experiencia en la ***Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales***, disponible en el sitio web del INAI, en la sección de Seguridad de los datos personales.

La ley platicada: El deber de seguridad

La Ley en su artículo 19, señala que **todo sujeto regulado que use datos personales debe establecer y mantener en el tiempo, controles de seguridad para proteger los datos que estén en su posesión.** Esto se detalla en el **Capítulo III del Reglamento de la Ley: De las Medidas de Seguridad en el Tratamiento de Datos Personales.** Asimismo, el INAI emitió en el Diario Oficial de la Federación las **Recomendaciones en Materia de Seguridad de Datos Personales**, las cuales parten de la premisa de que **la seguridad depende del entendimiento y conocimiento de los procesos donde se traten datos personales**. Es decir, si sabemos dónde y cómo recabamos, almacenamos, utilizamos y eliminamos la información, entonces sabremos dónde necesitamos establecer medidas de seguridad.

El Manual te ayudará a entender cómo tratas los datos personales y qué hacer **para cumplir con el deber de seguridad.**

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

- La protección de datos personales es un derecho humano de los titulares de los mismos y una obligación para quienes los utilizan.
- Ayuda a prevenir y mitigar los efectos de una fuga y/o mal uso de los datos personales.
- Evita afectaciones económicas debido a multas, compensación de daños y pérdida de clientes e inversionistas.
- Aumenta la competitividad, mejora los procesos de la organización y el nivel de confianza de los consumidores, inversionistas y titulares.

Más allá de minimizar el posible impacto económico por la imposición de sanciones por parte de la autoridad, el principal beneficio de establecer medidas de seguridad, documentarlas y mantenerlas, radica en el aumento de la certidumbre y confianza de los titulares de los datos personales. Al mismo tiempo, se aumenta la competitividad del mercado en general, se mejoran los procesos de la organización y la eficiencia y se facilita la inversión, incluso desde otros países.

2.2 Principales obligaciones para la protección de los datos personales

La ley platicada: El principio de responsabilidad

El Reglamento de la Ley en su artículo 47 establece como uno de los principios para la protección de datos personales, el de responsabilidad, que señala que **toda persona física o moral que trate datos personales tiene la obligación de velar por su resguardo y uso adecuado.**
Para ello, se debe **comenzar por poner orden en los procesos** y documentar los procedimientos.
Algunas medidas para cumplir con este procedimiento, de acuerdo con el artículo 48 del Reglamento de la Ley, son la elaboración de políticas y programas de privacidad, el análisis de los riesgos a la privacidad en nuevos productos, las revisiones periódicas, entre otros.

¡Todo dato personal tiene valor!

La Ley establece como uno de sus objetivos el **tratamiento legítimo** de los datos personales, lo que implica, entre otras cosas, que **los datos se deben utilizar sólo para las finalidades que el titular ha consentido al entregar su información**, por ejemplo para recibir un bien o servicio.

Importante: El aviso de privacidad

El aviso de privacidad es el medio por el cual los responsables de datos personales informan a los titulares el cómo y para qué usaran sus datos personales, y su elaboración y puesta a disposición es una de las obligaciones principales de todo aquél que utilice datos personales. Para mayor información y herramientas para elaborar un aviso de privacidad, puedes visitar el sitio web del INAI.

Esta obligación se debió de cumplir desde el 6 de julio de 2011.

El mantenimiento de forma segura de los sistemas a través de los que se obtienen, almacenan, procesan y/o comparten datos personales, puede ser una tarea compleja, que requiere tiempo, recursos y conocimientos especializados. Sin embargo, **esta tarea se facilita cuando quien trata datos personales identifica adecuadamente el uso de la información en cada uno de los procesos de su organización o negocio**, y este Manual le ayudará a esa tarea.

Si requiere conocer más sobre sus obligaciones en materia de protección de datos personales, puede consultar la guía del INAI sobre cumplimiento de obligaciones de la Ley.

2.3 Los riesgos a los que están expuestos los datos personales

Duda razonable: ¿De quién o de qué protejo los datos personales?

El propósito es protegerlos contra incidentes, es decir, cuidarlos de que una amenaza, (como el fuego o un ladrón) aproveche o explote una vulnerabilidad (por ejemplo la falta de extintores o la falta de cerraduras en puertas), y ocurra una vulneración de seguridad (pérdida de los datos personales por incendio o robo).

El riesgo es un concepto que puede entenderse como la probabilidad de que ocurra un incidente y su consecuencia desfavorable.

El objetivo de implementar medidas de seguridad es que cada una de ellas ayude a reducir el riesgo de que se materialice un incidente y sus consecuencias desfavorables. Las medidas de seguridad también ayudan a que, en caso de que se presente un incidente, se reduzca el daño a los titulares y a la empresa u organización.

La ley platicada: Tipos de vulneraciones

El Reglamento de la Ley en su artículo 63 establece que existen cuatro tipos de vulneraciones de seguridad a los datos personales, que pueden ocurrir en cualquier momento del tratamiento de información personal:

Es importante identificar los distintos orígenes que tienen los riesgos a los que están expuestos los datos personales, por ejemplo:

Amenazas por atacantes, es decir, hay riesgos que derivan de actividades humanas que tienen un objetivo previamente determinado. Por ejemplo, hackers, espías, competidores en busca de bases de datos de forma ilegal, entre otros.

Amenazas que son generadas a raíz de una situación fortuita en la que la vulneración puede darse sin que ésta haya sido planeada. Por ejemplo, un empleado de un laboratorio que suele prestar su computadora, corre el riesgo de que alguien copie desde el escritorio de su computadora a una memoria USB, el archivo "Pacientes con VIH.xls" el cual contiene datos personales sensibles.

Amenazas por descuido o desastre natural. Por ejemplo, la eliminación o modificación de un expediente por error humano, por falla en las computadoras, o pérdida de información a causa de un terremoto, inundación o incendio.

Casos de la vida real: El riesgo de los datos personales en custodia del Dr. Pérez

El Consultorio del Dr. Pérez se ha ganado la confianza de sus pacientes y se ha hecho de una buena reputación debido a que respeta la privacidad y confidencialidad de los datos personales de sus clientes, sobre todo después de la vulneración a la base de datos en custodia del Dr. Gómez, quien vendió los datos personales de sus pacientes a distintos despachos de venta de seguros. Por este hecho, la mayoría de los clientes del Dr. Gómez han decido cambiarse de médico, para ser atendidos por el Dr. Pérez.

Para disminuir la probabilidad de que ocurran vulneraciones, el Dr. Pérez se ha dado a la tarea **de identificar posibles incidentes** como:

Tipo de VULNERACIÓN	INCIDENTE
La pérdida o destrucción no autorizada de los expedientes	Que una persona mal intencionada *destruya los archivos físicos o electrónicos* que contienen los expedientes de sus pacientes, lo cual impediría otorgarles una adecuada atención, por ejemplo al atender sus solicitudes de derechos ARCO o ante una emergencia.
El robo, extravío o copia no autorizada	Que el Dr. Pérez extravíe su equipo de cómputo personal donde almacena los datos de sus pacientes y que caiga en manos de alguien que pueda hacer una *copia no autorizada de la base de datos*.
El uso o acceso no autorizado	Que la asistente del Dr. Pérez no bloquee la computadora de la recepción cuando va al baño, y que como consecuencia, un paciente curioso se acerque y pueda acceder a los archivos.
El daño, alteración o modificación no autorizada	Que alguien malintencionado altere un expediente de algunos pacientes del Dr. Pérez, modificando los padecimientos que tienen, por lo que podría recetar medicamentos y tratamientos inadecuados para cada persona.

Para ello, el Dr. Pérez llevará a cabo la implementación de acciones de seguridad que atiendan las amenazas que podrían causar estas vulneraciones.

Aprendizaje

Interesado en realizar un tratamiento responsable de la información personal y **tomando en cuenta los incidentes que otros han sufrido**, el Dr. Pérez ha **visualizado algunas amenazas que podrían causar una vulneración** a los datos personales que custodia, con estos escenarios en mente, le será más fácil implementar medidas de seguridad.

En el **Anexo C de la Guía** se proporcionan otros ejemplos de vulneraciones a la seguridad de los datos personales.

3. ¿Cómo aseguro los datos personales bajo mi custodia?

Ahora que conocemos la importancia de tener medidas de seguridad y su relación con el adecuado tratamiento de datos personales, **podemos continuar con la identificación de cada una de las etapas del proceso, que permitirán a los responsables y encargados elevar el nivel de seguridad y reducir el riesgo de sufrir una vulneración.**

La ley platicada: Acciones para la seguridad

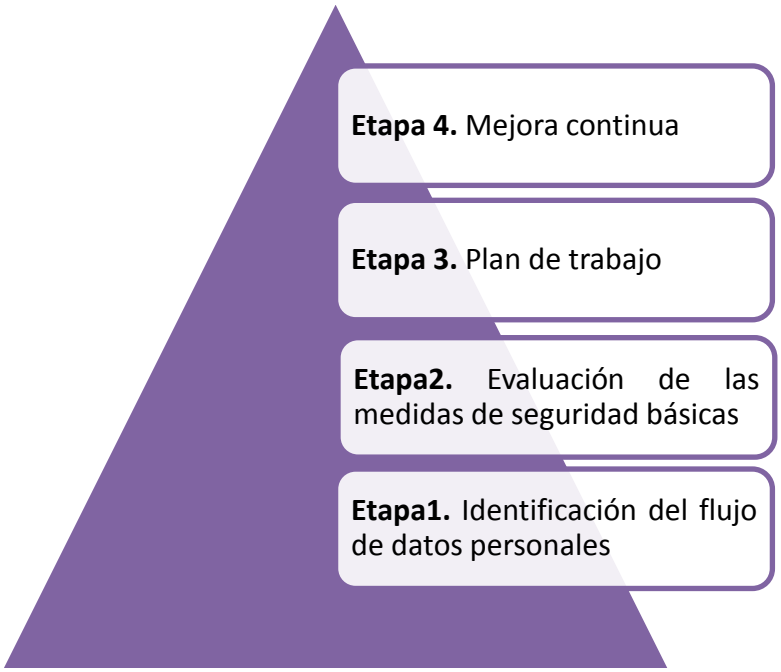
El Reglamento de la Ley en su artículo 61 establece las siguientes acciones para la seguridad de los datos personales:

1) Elaborar un inventario de datos y de sus medios de almacenamiento.
2) Determinar las funciones y obligaciones de las personas que traten datos personales.
3) Realizar un análisis de riesgos de los datos personales.
4) Revisar las medidas de seguridad existentes.
5) Realizar un análisis de brecha entre las medidas de seguridad existentes y las necesarias.
6) Elaborar un plan de trabajo para implementar las medidas de seguridad requeridas.
7) Realizar revisiones y auditorías del tratamiento de los datos y de las medidas de seguridad.
8) Mantener capacitado al personal relacionado con el tratamiento de los datos.

A través del Manual, los responsables y encargados de las micro, pequeñas y medianas empresas, así como de las organizaciones pequeñas, identificarán elementos de apoyo para cubrir cada una de estas acciones y así generar un esquema de seguridad continuo, consistente y efectivo.

Importante: Las etapas para madurar en la seguridad

Hay cuatro etapas que los responsables y encargados deberán alcanzar para madurar en el tema de seguridad de la información:



Como se representa en el diagrama, las etapas son acumulativas y no se puede avanzar a la siguiente sin cubrir adecuadamente la anterior.

La implementación de medidas de seguridad es un proceso que se debe hacer paulatina y secuencialmente, a fin de elegir controles útiles para mitigar el riesgo, optimizar tiempo y dinero y reforzar la seguridad de los datos personales cada vez más.

Etapa 1. Identificación del flujo de los datos personales

Los responsables y encargados deberán contestar cada una de las preguntas de esta etapa para **identificar con claridad el uso que dan a los datos personales, desde que los recaban hasta que los eliminan** en sus organizaciones o empresas.

Pregunta 1. ¿Qué tipos de datos personales recabo?

El objetivo es identificar qué tipo de datos personales se recaban en los distintos formatos que se utilizan y lo más importante, si es necesario recabarlos o no, con el fin de utilizar sólo los tipos de datos necesarios para la finalidad del servicio.

La respuesta a esta pregunta debe ser un listado de todos **los tipos de datos personales** que son **necesarios** para que la empresa pueda ofrecer productos y/o brindar servicios.

Casos de la vida real: Datos personales que recaba el Dr. Pérez

Mediante un aviso de privacidad el Dr. Pérez informa a sus pacientes sobre qué datos recaba y las finalidades relacionadas con su uso: mantenimiento del expediente médico, seguimiento a los padecimientos y tratamientos, historial de citas y el cobro de honorarios por consulta.

A continuación, **el Dr. Pérez realiza un listado de todos los tipos de datos que recaba a través de los diferentes formatos y al terminar, realiza una evaluación para saber si realmente utiliza esos datos** de acuerdo a las finalidades previstas en su aviso de privacidad, obteniendo una tabla como la siguiente:

Datos personales recabados	**Existente**	**Necesario**	**No necesario**
Datos de identificación			
Nombre	X	X	
Domicilio	X	X	
Teléfono de casa y/o celular	X	X	
Edad	X	X	
Sexo	X	X	

RFC	X	X	
Estado Civil	X		X
Datos personales sensibles			
Información médica y/o del estado de salud física y/o mental	X	X	
Opiniones y/o preferencias políticas	X		X

En su análisis, el Dr. Pérez identifica que almacena en sus registros **el estado civil** y **preferencias políticas** de sus pacientes, los cuales no son relevantes para el servicio que presta, por lo que decide tomar las siguientes acciones al respecto:

- Dejar de solicitar a sus pacientes estos datos innecesarios.
- Eliminar de la base de datos actual los registros que refieren a estos datos.
- Avisar a sus clientes sobre los cambios en el aviso de privacidad.

Las empresas y organizaciones podrían incluso, darse cuenta de que no requieren ciertos medios de almacenamiento y así eliminarlos.

Con estas acciones el Dr. Pérez podrá canalizar mejor sus esfuerzos en beneficio de la protección de los datos personales, pues no tendrá que almacenar datos que no requiere para la finalidad de sus servicios, y así disminuirá el nivel de riesgo al que expone a los titulares y cumplirá con el principio de proporcionalidad de la Ley. Se recomienda consultar la guía del INAI sobre cumplimiento de obligaciones de la Ley**.**

También se deberá tener cuidado y atención en la forma en que se obtienen los datos, por ejemplo el Dr. Pérez puede pedir nombre, teléfono y dirección de sus pacientes sin necesidad de solicitarles un comprobante de domicilio el cual podría contener datos innecesarios.

En el **Anexo A.1** se proporciona un listado general de los tipos de datos en un formato similar al utilizado por el Dr. Pérez para que las empresas y organizaciones elaboren sus propias listas de tipos de datos.

Importante: Sitios, Medios y Formatos

Para facilitar la identificación del ciclo de vida de los datos personales, se proponen las siguientes definiciones:

Sitio de resguardo: toda locación donde se resguarden los medios de almacenamiento, tanto físicos como electrónicos (por ejemplo, la casa, la empresa o las instalaciones de un tercero).

Medio de almacenamiento físico: es todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales, por ejemplo los expedientes de personal almacenados en un archivero. En este sentido hay que considerar cuartos especiales, bóvedas, muebles, cajones y cualquier espacio donde se guarden formatos físicos, o bien equipo de cómputo u otros medios de almacenamiento de datos personales.

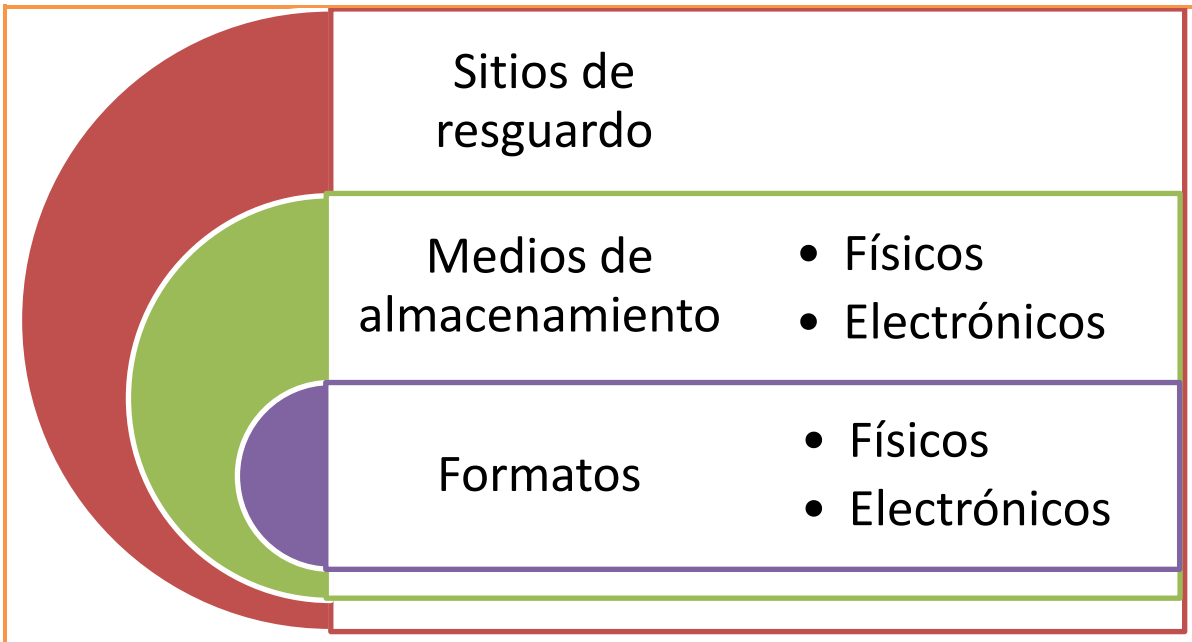
Medio de almacenamiento electrónico: es todo recurso al que se puede acceder sólo mediante el uso de equipo de cómputo que procese su contenido para examinar, modificar o almacenar los datos personales. Podemos considerar por ejemplo, discos duros (tanto los propios del equipo de cómputo como los portátiles), memorias extraíbles como *USB o SD, CDs, Blu-rays*, entre otros. También podemos contemplar como medio de almacenamiento electrónico, el uso de servicios de almacenamiento en línea.

> **Equipo de cómputo:** Cualquier dispositivo electrónico que permita el procesamiento de información por ejemplo, computadoras de escritorio, laptops, tabletas, teléfonos inteligentes, entre otros.

Formato físico: Es el documento físico o impreso que define cómo se obtiene la información personal, por ejemplo: un formulario, un contrato, la correspondencia, entre otros.

Formato electrónico: Es el mecanismo electrónico que define cómo se obtiene la información personal, por ejemplo un formulario de captura en procesador de texto, una hoja de cálculo o una base de datos.

La idea de estas definiciones es proporcionar un modelo que permita identificar el almacenamiento de la información personal de lo particular a lo general, como se muestra en la siguiente figura:



En este ejemplo, a través de los formatos físicos y electrónicos se obtienen los datos personales, que se resguardan en los medios de almacenamiento, los cuales a su vez se encuentran en los sitios de resguardo, de esta manera se documentará el modelo, conforme se contestan las preguntas 2 y 3.

Este modelo nos permite implementar medidas de seguridad por capas: el primer filtro para acceder a los datos personales es un sitio de resguardo, por ejemplo, una oficina con sistema de alarma, el siguiente filtro es el acceso al medio de almacenamiento, por ejemplo, un archivero bajo llave con los expedientes de los pacientes, y finalmente el acceso al formato, por ejemplo, los documentos que componen el expediente de un paciente en específico.

Pregunta 2. ¿Cómo recabo los datos personales?

El objetivo es identificar en qué tipo de formatos se recaban y almacenan los datos personales por el responsable.

La respuesta a esta pregunta debe ser un listado de todos los documentos, plantillas, formularios, físicos o electrónicos en los que se registran los datos personales identificados en la Pregunta 1.

Casos de la vida real: Cómo almacena el Dr. Pérez los datos personales

El Dr. Pérez realiza un análisis del cómo están agrupados los datos personales y en qué formatos se utilizan en el consultorio, luego los captura en una tabla como la que se muestra a continuación:

Formato	**Físico**	**Electrónico**
Correspondencia/Correo	Correspondencia de proveedores que llega al buzón postal del consultorio	Mensajes, carpetas y documentos de pacientes/proveedores, enviados y recibidos de la cuenta: drperez@correo.mx
Formularios	Formato impreso que se entrega a los nuevos pacientes para llenar	
Facturas		Documentos de tipo nombre_factura.pdf
Hojas de cálculo		Archivos: provedores.xls y pacientes.xls
Contratos	Impresiones de los contratos	Documentos de tipo: nombre_contrato.pdf o nombre_contrato.doc
Expedientes	Impresiones de los expedientes	Documentos de tipo: nombre_paciente.doc
Audio y/o Video		Videos de vigilancia de la cámara en recepción.

Con este análisis, el Dr. Pérez identificó a simple vista, que en los **formatos electrónicos** es en donde se **concentra mayor información personal** y también sabe que los **correos, hojas de cálculo y expedientes** son los medios de almacenamiento en los que maneja **mayor volumen de datos.**

Así como el Dr. Pérez, **las empresas y organizaciones deben ser capaces de identificar todos los formatos que utilizan para recabar y almacenar información personal**.

En el **Anexo A.2** se proporciona una tabla en blanco similar a la del Dr. Pérez para que las organizaciones elaboren sus propias listas de formatos de almacenamiento.

Pregunta 3. ¿Dónde se almacenan los datos personales?

Cada formato identificado puede estar almacenado en una o más ubicaciones, físicas o electrónicas.

La respuesta a esta pregunta debe ser un listado de los lugares, gabinetes, archiveros, carpetas, computadoras, etc. donde se almacenen los medios identificados en la Pregunta 2.

Casos de la vida real: ¿Dónde almacena el Dr. Pérez los datos personales?

Una vez que el Dr. Pérez ha identificado los formatos de almacenamiento, entonces procede a realizar un listado de los sitios y medios donde dichos formatos son guardados o utilizados. El Dr. Pérez comienza por identificar, de lo general a lo particular, los sitios donde almacenan medios como computadoras o archiveros, y después va identificando los contenedores más específicos, obteniendo una tabla como la que se muestra a continuación:

Sitios de resguardo	**¿Qué medios de almacenamiento se resguardan?**
Oficinas del Consultorio	Computadora de escritorio, archiveros, escritorios/cajones
Oficina en casa	Computadora portátil, escritorios/cajones
Medios de almacenamiento físico	**¿Qué formatos o medios de almacenamiento se resguardan?**
Cajones del Escritorio	Correspondencia postal, memorias *USB, CD´s, DVD´s*
Estantes/Archiveros	Formato impreso que se entrega a los nuevos pacientes para llenar, impresiones de los contratos, impresiones de los expedientes
Medios de almacenamiento electrónico	**¿Qué formatos de almacenamiento electrónico se resguardan?**
Computadoras de escritorio	Correos y carpetas de almacenamiento de documentos de la cuenta: drperez@correo.mx, archivos: provedores.xls y pacientes.xls, documentos de tipo: nombre_contrato.pdf o nombre_contrato.doc, documentos de tipo: nombre_paciente.doc, videos de vigilancia de la cámara en recepción
Computadoras portátiles (Laptop)	Correos y carpeta de almacenamiento de documentos de la cuenta: drperez@correo.mx, archivos: provedores.xls y pacientes.xls, documentos de tipo: nombre_contrato.pdf o nombre_contrato.doc, documentos de tipo: nombre_paciente.doc

Teléfonos inteligentes, tabletas y otros dispositivos móviles	Correos y carpeta de almacenamiento de documentos de la cuenta: drperez@correo.mx
Memorias USB, discos duros extraíbles y otros medios de almacenamiento electrónico	Archivos: provedores.xls y pacientes.xls
Almacenamiento en línea/Cómputo en la nube	Correos y carpeta de almacenamiento de documentos de la cuenta: drperez@correo.mx

Para elaborar esta lista el Dr. Pérez consideró todas las ubicaciones donde suele trabajar y las tareas que realiza en cada lugar. Una empresa u organización podría identificar que almacenan diferentes medios en múltiples lugares. **Reducir el número de sitios y medios utilizados para guardar información es un mecanismo para disminuir el riesgo.**

También es importante considerar carpetas físicas o electrónicas específicas. Por ejemplo, el Dr. Pérez podría tener todos sus documentos electrónicos relacionados con la atención a pacientes en la carpeta "Mi Consultorio" de la computadora de escritorio y hacer una copia de respaldo de esa carpeta en un disco duro externo, para después resguardarlo en la caja fuerte de su casa. Así evitaría tener información de esa carpeta en la computadora portátil o en cualquier otro lugar.

En el **Anexo A.3** se proporciona una tabla en blanco similar a la del Dr. Pérez para que las organizaciones elaboren sus propias listas de sitios y medios de almacenamiento.

Dato útil: Cómputo en la nube

El cómputo en la nube es un modelo de prestación de servicios, el cual permite a los clientes acceder a un conjunto de recursos de cómputo conforme a sus **necesidades de consumo**, desde el arrendamiento de infraestructura, hasta la utilización de software, todo a través de Internet, esto incluye, por ejemplo, cuentas de correo electrónico, almacenamiento de datos en línea, servicios de redes sociales y en general **cualquier servicio que pueda utilizarse desde un navegador de Internet**.

Aunque los servicios y aplicaciones de cómputo en la nube pueden proveer altos estándares de privacidad y seguridad de la información; al igual que otros servicios y aplicaciones, su nivel de seguridad depende de los términos de uso o del contrato de servicio, así como de la configuración que defina el usuario, por lo que es muy recomendable atender las medidas de seguridad en el entorno de trabajo digital descritas en esta guía.

Pregunta 4. ¿Quién tiene permiso para acceder o manejar los datos personales?

Diferentes personas en una empresa u organización pueden tener acceso a los sitios donde se almacenan los datos personales. Las personas identificadas y autorizadas para acceder podrían manejar la información personal con permisos específicos de uso, esto es conocido comúnmente como un esquema de privilegios.

La respuesta a esta pregunta es una relación de las personas que tienen acceso autorizado a los sitios identificados o permisos para manejar los medios que contienen datos personales en la Pregunta 3.

Casos de la vida real: ¿Quién accede o maneja los datos personales en custodia del Dr. Pérez?

Con la identificación de todos los sitios y medios, **el Dr. Pérez elabora una lista de privilegios para documentar el acceso o manejo que tienen él y su asistente a los datos personales**, en una tabla como la que se muestra a continuación:

Sitios de resguardo	**¿Quiénes tienen privilegios de acceso?**
Oficinas del Consultorio	Dr. Pérez, Asistente
Oficina en casa	Dr. Pérez
Medios de almacenamiento físico	**¿Quiénes tiene privilegios de acceso?**
Escritorios/Cajones del Consultorio	Dr. Pérez, Asistente
Archiveros	Dr. Pérez, Asistente
Medios de almacenamiento electrónico	**¿Quiénes tienen privilegios de uso?**
Computadoras de escritorio	Dr. Pérez, Asistente
Computadoras portátiles (Laptop)	Dr. Pérez
Teléfonos inteligentes, tabletas y otros dispositivos móviles	Dr. Pérez
Memorias USB, discos duros extraíbles y otros medios de almacenamiento	Dr. Pérez, Asistente

electrónico	
Almacenamiento en línea/Cómputo en la nube	Dr. Pérez
Formatos de almacenamiento electrónico	**¿Quiénes tienen privilegios de uso?**
Documentos de tipo: nombre_paciente.doc	Dr. Pérez, Asistente

Para los privilegios de acceso el Dr. Pérez no sólo enlista los sitios que tiene identificados, sino aquellos medios de almacenamiento y formatos que deban tener un acceso restringido. Por ejemplo, tanto el Dr. Pérez como su asistente tienen acceso a la computadora de escritorio de la oficina, pero los documentos de tipo *nombre_paciente.doc*, deben estar restringidos sólo para ser vistos y modificados por el doctor, **por lo que en adelante restringirá el acceso a estos archivos a su Asistente**. **La idea detrás de revisar los privilegios, es identificar quienes tienen acceso a los datos y controlar su tratamiento.**

Los **Anexos A.2 y A.3** proporcionan tablas en blanco similares a las del Dr. Pérez para que las organizaciones elaboren sus propias listas de privilegios de acceso.

Antes de pasar a la siguiente etapa conviene volver a contestar las preguntas previas para asegurarse de que no se han realizado omisiones en la identificación de los datos personales durante su tratamiento y en su caso, realizar las preguntas correspondientes para identificar las medidas necesarias.

Casos de la vida real: El Dr. Pérez, revisando los datos personales que maneja una vez más

Al revisar por segunda ocasión sus archivos, el Dr. Pérez se ha dado cuenta que **también tiene en su poder los expedientes de los pacientes que han dejado de visitarlo,** por lo que deberá protegerlos de la misma forma en que cuide los de sus pacientes actuales, en el entendido de que solamente se resguardan para cumplir con las regulaciones vigentes y que no son utilizados para ningún otro fin.

Por otro lado, el Dr. Pérez notó que algunos prospectos que proporcionaron sus datos de identificación, enfermedades y padecimientos en una expo **no le firmaron el aviso de privacidad utilizado para otorgarle el consentimiento expreso** para utilizar sus datos. Por lo que, tendrá que contactarlos para poner a su disposición el aviso y solicitarles su consentimiento expreso. Después de esto, deberá destruir aquellos datos de los titulares que hayan decidido no dar su consentimiento.

Resumen de la Etapa 1
¿Qué ha hecho el Dr. Pérez hasta este momento?

El Dr. Pérez en esta etapa logró identificar y documentar:

- ☑ Los **tipos de datos** que utiliza, con lo que podrá evitar el uso de los datos innecesarios.
- ☑ Los **medios** y **formatos** en los que recaba y almacena los datos personales.
- ☑ Los **sitios** donde resguarda los datos personales.
- ☑ Los **privilegios** de acceso/uso a los sitios, medios y formatos de almacenamiento.

Etapa 2. Evaluación de las medidas de seguridad básicas

Importante: Entornos de trabajo

Las actividades de una empresa u organización pueden desarrollarse en ambientes físicos y digitales, así que para esta sección, debemos considerar las siguientes definiciones:

Entorno de trabajo físico: Cualquier lugar físico donde se desarrollen actividades de la empresa u organización, por ejemplo, las oficinas de la empresa u organización, la casa, oficinas de otra empresa u organización, una mesita en un café público, entre otros.

Entorno de trabajo digital: Es el ámbito conformado por la conjunción de hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permita el intercambio o procesamiento computarizado de datos, para el desarrollo de las actividades de la organización.

Para una organización, no es posible implementar un programa de seguridad de la información que reduzca el riesgo a cero, **sin embargo, se pueden poner en marcha medidas de seguridad básicas para minimizar las vulneraciones a la seguridad de los datos personales y sistemas de tratamiento.**

Las medidas de seguridad pueden abordarse bajo las siguientes categorías generales:

A) **Medidas de seguridad basadas en la cultura del personal.**
B) **Medidas de seguridad en el entorno de trabajo físico.**
C) **Medidas de seguridad en el entorno de trabajo digital.**

En esta etapa, los responsables y encargados del tratamiento de datos personales **deberán contestar Sí, No o No aplica, a las preguntas de la sección,** dependiendo de los medios y sitios identificados en la etapa 1.

A. Medidas de seguridad basadas en la cultura del personal

Una de las principales causas por las que ocurre robo o extravío de datos personales e incluso de cualquier información relevante para la organización, es simplemente porque los datos no se cuidan adecuadamente. El siguiente grupo de preguntas tienen como objetivo identificar las prácticas inadecuadas más comunes, que podrían provocar una vulneración a la seguridad.

A.1. ¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?

Cuando se dejan datos personales sin supervisión o por descuido, éstos corren el riesgo de ser sustraídos por alguien más (interno o externo a la organización). Por ello es importante considerar controles como:

A.1.1. Política de escritorio limpio: No dejar a simple vista documentos importantes, equipo de cómputo, contraseñas en *"post-it"*, llaves, identificaciones, entre otros.

A.1.2. Hábitos de cierre y resguardo: Esto debe incluir conductas como: que cada empleado cierre sus cajones, que las cosas importantes siempre se mantengan bajo llave si no están en uso y/o que el último en salir de las oficinas cierre los archiveros y las puertas con llave, y active las alarmas.

A.1.3. Impresoras, escáneres, copiadoras y buzones limpios: Nunca se deben dejar abandonados documentos en áreas de uso común como las mencionadas.

A.1.4. Gestión de bitácoras, usuarios y acceso: Para controlar el acceso a los sitios, medios de almacenamiento, formatos y equipo de cómputo, se puede hacer con bitácoras tan simples como una lista donde se anote el nombre, fecha y hora de la persona que accede a un archivero para consultar un expediente, o bien, llevar bitácoras automatizadas para el uso de medios electrónicos. Es importante habilitar los mecanismos de registro en los equipos de cómputo y su software para identificar la actividad de los usuarios. Así como revisar que las credenciales y permisos de los usuarios estén bien definidos.

A.2. ¿Tienes mecanismos para eliminar de manera segura la información?

Si cualquier documento es depositado simplemente en la basura, éste puede ser recuperado y visto por cualquier persona malintencionada, y así ocurrir una fuga de información importante. Por otra parte, en los medios electrónicos, **la simple acción de "borrado" no elimina de forma definitiva la información**, y ésta puede ser recuperada desde los dispositivos desechados, con ciertas herramientas. Por ello se deben tomar en cuenta controles como:

A.2.1. Destrucción segura de documentos: Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturado o incinerado. Cuando se adquiere equipo para estas tareas se debe evaluar que tan difícil sería para una persona recuperar la información, por ejemplo, hay trituradoras que hacen tiras el papel y otras que lo hacen pequeños trozos. Con tiempo y esfuerzo es posible recuperar un documento hecho tiras, pero es muy difícil recuperar uno hecho *"confeti"* o cenizas. Otra opción es almacenar en un sitio seguro los documentos a triturar y entregarlos periódicamente a alguien que preste el servicio de destrucción de documentos, sin olvidar que debe existir un contrato que estipule claramente el deber de confidencialidad del prestador de servicio.

A.2.2. Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico: Es conocido que en los equipos de cómputo se puede "borrar" o "eliminar" la información de forma simple o con un clic, pero debido a la naturaleza del almacenamiento electrónico, lo que ocurre en realidad, es que ésta deja de ser fácilmente accesible pero sigue ahí hasta que nueva información la *"sobrescribe"*. Para la eliminación definitiva de información existen herramientas de software que borran archivos electrónicos específicos o dispositivos de almacenamiento completos. Cuando la vida útil de un equipo de cómputo o medio de almacenamiento electrónico ha terminado, es recomendable destruirlo físicamente. Esto lo puede hacer la misma organización o contratar a un tercero para este servicio, cuando la cantidad de equipo de cómputo es mayor.

A.2.3. Fijar periodos de retención y destrucción de información: Es importante identificar de manera regular toda la información que ya no es de utilidad para la organización y que no requiere almacenarse para cumplir con alguna responsabilidad legal o contractual. Los procedimientos de eliminación de información de gran valor o a gran escala deben ser formales y se deben registrar en bitácoras.

A.2.4. Tomar precauciones con los procedimientos de re-utilización: Por diversas razones, las organizaciones pueden optar por diferentes mecanismos de reciclado para minimizar costos, pero se debe ser cuidadoso en la posible exposición de datos personales. Por ejemplo, es común el uso de "bandejas de papel reciclado", pero bajo ninguna circunstancia deberían utilizarse documentos con datos personales como "papel de reúso". Cuando el equipo de cómputo tenga que cambiar de dueño por ejemplo, de un empleado a otro, es importante respaldar la información relevante para la organización y borrar completamente los datos que resguarda el equipo.

A.3. ¿Has establecido y documentado los compromisos respecto a la protección de datos?

Todos aquellos involucrados en el tratamiento de datos personales deben actuar con relación a los principios que establece la Ley. **No se deben obviar o dejar como reglas implícitas todas aquéllas relacionadas a la privacidad y protección de datos personales de las personas.** De manera adicional, se debe fomentar la cultura de la seguridad y la noción del valor intrínseco de la información. Por ello, se deben considerar estrategias como:

A.3.1. Informar al personal sobre sus deberes mínimos de seguridad y protección de datos: El personal involucrado en el tratamiento de datos personales debe estar informado de manera explícita que tiene un compromiso y responsabilidad sobre la información en su custodia, y en su caso tareas específicas a realizar. Esto incluye por ejemplo, informar al personal de nuevo ingreso sobre sus funciones y obligaciones para la protección de datos e incluir cláusulas al respecto cuando se hace una contratación. En su caso, también se debe informar a los empleados de las posibles consecuencias y medidas disciplinarias relacionadas, en caso de no cumplir con sus deberes.

A.3.2. Fomentar la cultura de la seguridad de la información: En el trabajo diario, es común que a todas las personas que manejan información personal de manera continua, se les vuelva una actividad rutinaria, esto puede provocar que sean descuidados con la gestión de la información. Por lo que es necesario permear la seguridad de la información como una práctica cotidiana, recordando la importancia de este deber e incentivando a los empleados, para que entre ellos se recuerden el uso de medidas de seguridad y buenos hábitos de tratamiento.

A.3.3. Difundir noticias en temas de seguridad: Mantener informado al personal respecto a las últimas noticias en seguridad puede parecer complejo, sin embargo existen muchos medios de comunicación, como las redes sociales, por los cuales las organizaciones se pueden mantener al tanto de las historias más relevantes en seguridad.

A.3.4. Prevenir al personal sobre la *Ingeniería Social*: De manera general se considera a la ingeniería social como un conjunto de técnicas para influenciar a una persona a tomar acciones que pueden estar o no dentro de sus intereses o responsabilidades. Estas técnicas pueden ser utilizadas por criminales para engañar a personas desprevenidas en línea, por teléfono o personalmente. Se debe invitar al empleado a que sea "cauto y cortés" es decir, que se cuestione en todo momento si alguna solicitud tiene sentido y si está dentro de sus responsabilidades cumplirla, de lo contrario negarse educadamente a entregar la información o a realizar la acción solicitada e informar de este hecho a su jefe inmediato.

A.3.5. Asegurar la protección de datos personales en subcontrataciones: La organización no debe asumir que un proveedor o cualquier externo tomará las medidas de seguridad necesarias para proteger la información personal y que la tratará como confidencial, sin que esto se manifieste explícitamente. Por ejemplo, a través de cláusulas que especifiquen claramente el tratamiento legítimo y las medidas de seguridad implementadas para la protección de los datos personales. Otros tipos de convenio que deben revisarse son los relacionados a la compra, venta o intercambio de datos de titulares, revisando a detalle que los datos sean utilizados con el consentimiento del titular. Además, en el uso de servicios de almacenamiento en línea o de cómputo en la nube, por ejemplo, el correo electrónico, se debe revisar y evaluar si el contrato de adhesión garantiza seguridad y confidencialidad de los datos que se almacenen.

A.4. ¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?

Para las organizaciones, incluso para aquéllas con gran madurez en el tema de seguridad de la información, **el tema de vulneraciones a la seguridad de los datos personales puede resultar particularmente complicado, la idea básica es disminuir la afectación a los titulares** de los datos personales y a la organización. Por eso, se requiere tomar medidas como:

A.4.1. Tener un procedimiento de notificación: Se debe tener establecida una cadena de avisos dentro de la empresa u organización en caso de que ocurra una vulneración a la seguridad. Cuando un empleado sufra o identifique un incidente de seguridad, éste debe tener muy claro a quién debe avisar en la empresa u organización. El responsable debe evaluar qué

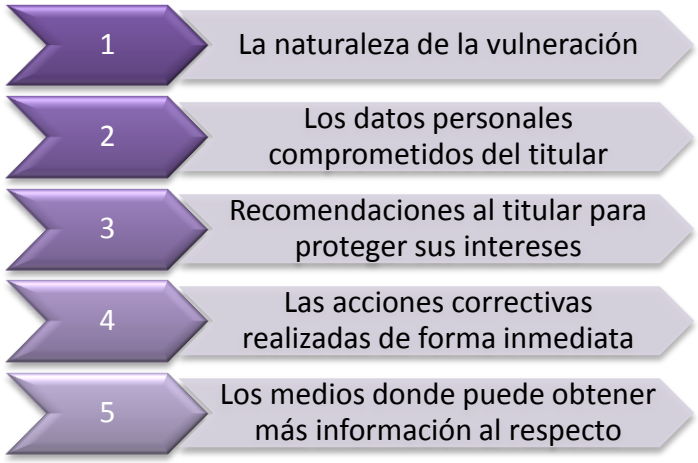
información se afectó y los medios para notificar a los titulares de lo ocurrido, esto con el fin de alertarlos y que tomen precauciones.

Adicionalmente, se podrá diagnosticar el posible impacto a las operaciones y tomar acciones que mitiguen el incidente, por ejemplo actualizando sus procedimientos y medidas de seguridad.

A.4.2. Realizar revisiones y auditorías: Se debe considerar la revisión periódica a la empresa u organización por un especialista en temas de seguridad para que éste realice evaluaciones y recomendaciones. Por la naturaleza técnica de algunas amenazas, este tipo de revisiones podrían ayudar a revelar malas prácticas en el tratamiento de datos personales o la existencia de vulneraciones a la seguridad no detectadas, por ejemplo a través de las llamadas pruebas de penetración o *pentest.* Los resultados de cualquier evaluación deben informarse a los empleados involucrados en el tratamiento de datos personales.

La ley platicada: Notificación de vulneraciones a la seguridad de los datos personales

El Reglamento de la Ley establece que el responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado acciones para reducir la posible afectación a los titulares. La notificación a los titulares debe considerar al menos:



A.5. ¿Realizas respaldos periódicos de los datos personales?

En la medida de lo posible se deben almacenar los documentos físicos en medio electrónico, es decir, capturar, digitalizar o escanear la información en papel para almacenarla, de forma tal que se resguarde el mínimo de información en papel y sólo se imprima cuando sea estrictamente necesario. Esto debido a que es más práctico respaldar información copiando un archivo de un medio electrónico a otro, comparado con fotocopiar, organizar y almacenar documentos en papel.

Los datos personales almacenados en equipo de cómputo pueden dañarse de manera parcial o total debido a fallas en los sistemas o aplicaciones, por errores de operación de las personas, o bien por interrupciones de energía eléctrica, si se realizan respaldos de la información importante de manera periódica pueden mitigarse las consecuencias de estos incidentes. Es importante que los respaldos se realicen de manera regular y también cada vez que haya una actualización importante de los datos que están siendo almacenados en la organización. Se pueden realizar respaldos parciales sólo de la información crítica, diario o cada semana, y respaldos de toda la información, cada quince días o mensualmente. Es importante que los respaldos no se encuentren en la misma ubicación física que la información que se están respaldando y hacer pruebas de recuperación de las copias de respaldo para asegurarnos de que la información se encuentra íntegra.

B. Medidas de seguridad en el entorno de trabajo físico

Conforme los equipos de cómputo son cada vez más pequeños, ligeros y convenientes **se vuelve muy fácil para las personas llevar información con ellos**, por otro lado para muchas organizaciones es común revisar información en lugares públicos como un restaurante, cafetería o en el transporte público. La seguridad del entorno de trabajo físico es un elemento básico para mitigar vulneraciones a la seguridad de los datos personales.

B.1. ¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?

El acceso al entorno de trabajo físico debe ser sólo para personal autorizado, si no existen restricciones para el acceso, se corre el riesgo de que los datos personales sean robados o manipulados. De manera particular, **ninguna persona sin autorización debería poder acercarse al equipo de cómputo, archiveros con datos personales, o a cualquier otro medio de almacenamiento.** Para esto se deben considerar medidas como:

B.1.1. Alerta del entorno de trabajo: No se debe permitir que alguien sin motivos relacionados al funcionamiento del negocio ingrese al entorno de trabajo. Se debe tener precaución con las personas no autorizadas al entorno, por ejemplo, en las oficinas de la empresa u organización debería haber áreas como un mostrador de recepción o si se está trabajando en un café se debería evitar que alguna persona extraña esté muy cerca de los elementos donde se tengan datos personales. Siempre se debe cuestionar la presencia de un extraño sin acompañamiento o que se encuentre cerca del entorno de trabajo.

B.1.2. Mantener bitácoras del personal con acceso al entorno de trabajo: En entornos como oficinas es importante mantener un registro de todos los que ingresan y salen y acordar que

aquéllos que salen al final del entorno de trabajo deben poner especial atención, dicho de manera coloquial el “último en salir cierra”.

B.2. ¿Tienes medidas de seguridad para evitar el robo?

Se deben establecer **medidas con las cuales se minimice el riesgo de que alguien robe información** fácilmente. Por ejemplo:

B.2.1. Cerraduras y candados: En las oficinas de la empresa u organización o en casa se debe contar como mínimo con gavetas, escritorios, o archiveros que se puedan cerrar con llave. El mismo principio aplica para otros entornos, usando candados para laptops o maletas con cierre de combinación.

B.2.2. Elementos disuasorios: Existen medidas de seguridad que reducen de manera significativa el interés de un atacante, por ejemplo, alarmas (tanto para el entorno como para los dispositivos), guardias de seguridad, rejas, maletines de seguridad, entre otros.

B.2.3. Minimizar el riesgo oportunista: Es necesario limitar el número de entornos de trabajo donde se realice tratamiento de datos personales (por ejemplo, sólo en casa o en la oficina), si es necesario trabajar constantemente en otros entornos (como aeropuertos u oficinas de otros clientes) se debe permanecer especialmente cauto del entorno y nunca dejar un elemento con datos personales sin supervisión.

B.3. ¿Cuidas el movimiento de información en entornos de trabajo físicos?

Al realizar envío de información siempre se corre el **riesgo de que ésta se pierda o sea robada.** Por ello, es importante tener controles de seguridad **que minimicen el impacto del extravío,** como:

B.3.1. Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico: Se debe registrar el permiso o la acción relacionada a la salida de los elementos mencionados en una bitácora, esto con el fin de que, en caso de pérdida, robo, daño o extravío se tenga control del posible impacto.

B.3.2. Mantener en movimiento sólo copias de la información, no el elemento original: Un incidente común en las organizaciones de cualquier tamaño es que la información que se pierde es la única información disponible. La información que sale de los entornos de trabajo usuales debería ser una copia, y no la información original.

B.3.3. Usar mensajería certificada: Es importante que el envío físico de medios que contienen datos personales se realice con mensajería segura/certificada, o en su defecto con personal de confianza, y siempre se debe recabar el acuse de recibo del envío.

C. Medidas de seguridad en el entorno de trabajo digital

Muchas de las operaciones de las organizaciones y de los mismos titulares están siendo llevadas a entornos digitales, **por lo que se vuelve primordial proteger equipos de cómputo y dispositivos de almacenamiento contra el acceso no autorizado**, de igual forma, **contra amenazas informáticas** como **software malicioso (malware, virus, entre otros).**

Dato útil: Malware

Malware es la abreviatura de *"Malicious software"*, un **término que engloba a todo tipo de programa o código malicioso cuyas funciones pueden variar desde extraer, borrar e incluso "secuestrar" la información en equipos de cómputo o generar malfuncionamiento en los sistemas.** Pese a que se suele escuchar de diversas clasificaciones de código malicioso como virus, troyanos, gusanos, entre otros, en la actualidad y dado que la cantidad de estas amenazas crece día con día, no existe muchas veces una diferencia clara entre ellas.

C.1. ¿Realizas actualizaciones al equipo de cómputo?

Si una deficiencia en la seguridad de un equipo de cómputo (llamada vulnerabilidad o agujero) no es atendida, **el equipo puede infectarse con malware o tener algún malfuncionamiento.** Los productos de software como sistemas operativos, programas y aplicaciones deben encontrarse en sus versiones más recientes y/o debidamente actualizadas. La mayoría del equipo de cómputo de uso común y su software está configurado para actualizarse de manera periódica, sin embargo debe verificarse que efectivamente esté habilitada esta funcionalidad, de lo contrario se debe programar al menos una vez al mes un espacio para realizar las actualizaciones correspondientes.

C.2. ¿Revisas periódicamente el software instalado en el equipo de cómputo?

Es importante revisar periódicamente qué tipos de programas se encuentran instalados en el equipo de cómputo, para verificar que se esté utilizando sólo software autorizado y evitar la instalación de software no deseado. Es de especial importancia evitar el uso de software para "bajar" o compartir archivos en equipos de cómputo de la organización, o con otros dispositivos personales, como tabletas o celulares, no sólo para evitar infringir la ley de derechos de autor, sino porque este software puede dar acceso a la información de un equipo a personas malintencionadas. También se debe vigilar que no se tenga instalado software sin licencia o "pirata", ya que éste podría estar infectado o simplemente no operar como el original y causar pérdida de información.

C.3. ¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?

El equipo de cómputo es susceptible a que cualquiera lo pueda utilizar, incluso personal no autorizado. Se deben tomar medidas de seguridad para evitar que alguien use un equipo de

cómputo, medio de almacenamiento electrónico o acceda a un entorno de trabajo digital sin autorización, por ejemplo mediante el uso de contraseñas y/o cifrado, o de aplicaciones o dispositivos para la verificación de identidad del usuario.

Dato útil: BYOD, BYOC, BYO…

BYO corresponde a *Bring Your Own*, es decir "trae tu propio", así se puede escuchar de tendencias como:

- **BYOD (Trae tu propio dispositivo):** Es decir, **un empleado trae sus propios equipos de cómputo** y los utiliza para almacenar y tratar información en custodia de la organización.
- **BYOC (Trae tu propia nube):** Es decir**, un empleado utiliza almacenamiento en línea u otros servicios**, como el de su cuenta de correo personal o edición de documentos en línea, para extraer y tratar información de la organización.

Lo más recomendable para una empresa u organización es que delimite el uso de estas tendencias, destinando equipo de cómputo y/o almacenamiento en línea específico para las tareas de la organización, y si se requiere trabajar con recursos externos, se deben utilizar herramientas de software o mecanismos para separar la información que custodia la organización y tomar medidas de seguridad al menos iguales a las ya implementadas.

Por ejemplo el Dr. Pérez usa la cuenta drperez@correo.mx, enlazada a un *smartphone*, sólo para asuntos del consultorio. Para recibir mensajes personales usa otra cuenta de correo y aunque en su laptop realiza operaciones personales, lo hace con un usuario diferente.

C.3.1. Uso de contraseñas y/o cifrado: Toda información personal en medio digital debería estar protegida con bloqueos por contraseña y/o cifrado, para evitar su acceso no autorizado y posibles eventos de robo o pérdida de información.

Dato útil: Cifrado y Contraseñas

La mayoría de las personas están familiarizadas con el concepto de **contraseña: el uso de información secreta para tener acceso a un equipo de cómputo, archivo o servicio.**

Sin embargo, la noción de contraseña puede estar ligada a un mecanismo de seguridad de la información más potente, **el cifrado**, **que es un proceso mediante el cual la información se convierte a un formato ilegible para todo aquél que no posea la contraseña.**

Pensemos por ejemplo, en un *smartphone* con una pantalla de bloqueo por contraseña, si es robado, un ladrón en su primer intento, quizá no pueda acceder a la información del teléfono por no conocer la contraseña, pero podría conectar el teléfono a una computadora que lo reconocería como un dispositivo de almacenamiento, entonces el ladrón podría ver la información. **Si el teléfono estuviera cifrado, la información no sólo sería difícil de acceder, sería ilegible sin la contraseña.**

Muchos equipos de cómputo recientes cuentan con algún elemento en su configuración que permite cifrar su contenido, además existen herramientas de software para el cifrado de archivos, dispositivos de almacenamiento (como memorias USB) e incluso de la conexión a Internet (como las Redes Virtuales Privadas o VPN).

"Las contraseñas sólidas y el cifrado son las medidas de seguridad en equipo de cómputo y medios de almacenamiento más básicas y más poderosas"

C.3.2. Uso de contraseñas sólidas: Una contraseña débil es susceptible a ser *"crakeada"* es decir, averiguar la contraseña con herramientas de software o simplemente adivinando. Se debe evitar el uso de información personal o palabras simples en las contraseñas. Aunque es una recomendación usual el crear contraseñas mezclando caracteres especiales y números para hacerlas difícil de adivinar, también puede ser difícil para los usuarios memorizarlas, y provocar que recaigan en malas prácticas como tenerlas escritas a la vista. Una mejor alternativa puede ser el uso de *"passphrases"*, es decir, frases o ideas completas por ejemplo, "me gusta la pizza de jamón", esta es una contraseña segura por ser muy larga y difícil de adivinar, pero es fácil de aprender. Otra opción es usar software de administración de contraseñas.

C.3.3. Bloqueo y cierre de sesiones: Cuando no se utilice el equipo de cómputo se debe bloquear o cerrar la sesión de usuario. Si un equipo no se va a utilizar por un periodo largo, se debe optar por apagarlo. Todo inicio de sesión debe requerir el uso de una contraseña, *token,* u otro mecanismo de autenticación. También se pueden considerar mecanismos de bloqueo y borrado remoto para los dispositivos móviles, de forma tal que se pueda restringir o eliminar la información aun cuando un equipo haya sido robado o extraviado.

C.3.4. Administrar usuarios y accesos: Se debe minimizar el uso de credenciales compartidas, es decir, que más de una persona tenga acceso al mismo servicio con el mismo usuario y contraseña por ejemplo, que dos personas distintas usen la misma identificación para usar la misma cuenta de correo. En su caso, cuando se implementan sistemas de tratamiento más

complejos, por ejemplo bases de datos, se debe tener una correcta administración de los usuarios, contraseñas y privilegios de acceso (permisos para leer y modificar un archivo).

C.4. ¿Revisas la configuración de seguridad del equipo de cómputo?

El equipo de cómputo, el software y en algunas ocasiones los medios de almacenamiento electrónico tienen configuraciones que permiten incrementar su nivel de seguridad. Los responsables deben habilitar las opciones de seguridad que permita a sus equipos estar más seguros por ejemplo, encender el *firewall* o habilitar las actualizaciones automáticas del antivirus, esta práctica, conocida como *hardening* o endurecimiento, puede requerir de cierto estudio y dedicación. Sin embargo, gracias a lo amigable de las nuevas herramientas así como a la información disponible en los sitios de Internet para soporte en línea del fabricante o proveedor, esta tarea es más fácil y podemos incrementar el nivel de seguridad significativamente. Es conveniente que todos los equipos de la organización, ya sean fijos o portátiles, mantengan un mismo nivel de configuración de seguridad.

C.5. ¿Tienes medidas de seguridad para navegar en entornos digitales?

El uso cotidiano de los equipos de cómputo y de los entornos digitales **hace que se den por obvias algunas conductas que podrían representar riesgo a los datos personales**, por ello se deben implementar medidas de seguridad como:

C.5.1. Instalar herramientas antimalware y de filtrado de tráfico: el software malicioso o malware comprende diferentes tipos como virus, troyanos, gusanos, entre otros, que tiene por objetivo extraer datos de los usuarios como sus contraseñas o números de cuenta bancaria. Se debe instalar al menos, software antivirus y habilitar el filtrado de tráfico (como un *firewall).*

C.5.2. Reglas de navegación segura: Sólo se deben revisar sitios web esenciales para el negocio, evitando navegar en sitios no relacionados y mucho menos en sitios de riesgo como son los de descarga de contenido que violan los derechos de autor o pornográficos.

Todos los empleados deben estar informados de los riesgos a los que se exponen por visitar sitios web que no son relevantes para sus funciones, también se les debe informar del peligro relacionado a la descarga de contenido, y la ventaja de verificar que el protocolo de conexión a los sitios web sea seguro es decir, verificar que en la dirección web aparezca *https* y la imagen de un candado, en lugar de que sólo sea *http.* Además, se puede optar por herramientas de cifrado de las comunicaciones como las redes virtuales privadas (o VPN, *Virtual Private Network*).

C.5.3. Reglas para la divulgación de información: Antes de enviar información a un tercero, almacenarla en cuentas de cómputo en la nube, publicarla en un sitio web, o compartirla en redes sociales, se debe evaluar si esta acción no está poniendo en riesgo a titulares o a personal de la organización.

C.5.4. Uso de conexiones seguras: Además de verificar que los protocolos de navegación sean seguros, se debe cuidar que la conexión también sea confiable. Cuando se trate de redes

inalámbricas, éstas deberán contar con contraseñas y configuración segura (por ejemplo WPA o WPA2, evitando conectarse o configurar redes WEP o abiertas, susceptibles a que un externo malintencionado intercepte las comunicaciones).

Asimismo es preferible evitar el uso de redes públicas, particularmente en los casos en que sea necesario llevar a cabo una transacción que implique el uso de información personal o contraseñas (por ejemplo, acceder a un portal bancario mediante un dispositivo portátil, utilizando una red *WiFi* provista por un sitio público, como un aeropuerto o una cafetería). De manera general, si no se puede asegurar la conexión, se deberá evitar cualquier tratamiento que involucre datos personales en línea.

Dato útil: Puntos de acceso seguros

Cuando contratamos un servicio de Internet para nuestra casa u organización, generalmente se nos proporciona un dispositivo que servirá de punto de acceso para conectarnos, o bien podemos adquirir por nuestra cuenta un equipo *enrutador* (*router*) para tal propósito. **Estos dispositivos suelen integrar herramientas y configuraciones de seguridad,** como *firewalls*, traducción de direcciones de red (o NAT, *Network Address Translation*) y otras características que debemos activar, para proteger mejor la red frente a un tercero no autorizado.

Además, **se debe elegir cuidadosamente la ubicación del enrutador o el punto de acceso de su conexión a Internet.** Si el dispositivo se encuentra en un área de fácil acceso, es susceptible a que un tercero se conecte físicamente y modifique la configuración de seguridad. Por otra parte, las señales inalámbricas pueden alcanzar varias decenas de metros y, por lo tanto, la señal de su red puede difundirse fuera de los límites de su organización. Puede limitar el área de alcance de la señal inalámbrica colocando el enrutador o el punto de acceso en un lugar central de la organización, en lugar de ponerlo junto a una pared exterior o una ventana.

C.6. ¿Cuidas el movimiento de información en entornos de trabajo digitales?

El envío erróneo o intercepción de mensajes electrónicos (ya sea correo, mensajería instantánea, redes sociales, mensajes de texto a celular, entre otros) **representa una grave fuga de información que puede perjudicar seriamente a los titulares.** Es por esto que se debe considerar:

C.6.1. Validación del destinatario de una comunicación: Se han registrado muchos incidentes en los cuales la información personal se ha fugado a terceros debido a la transmisión errónea de mensajes electrónicos como correos, faxes, redes

sociales, entre otros. Antes de enviar un mensaje se debe asegurar que el envío se realiza al destinatario correcto. Cuando se envíe un mensaje electrónico a varios destinatarios se debe revisar el método de envío y designación (por ejemplo en correo electrónico, *CC o con copia*, *CCO o con copia oculta*).

C.6.2. Seguridad de la información enviada y recibida: Cuando se envía información importante a través de mensajes electrónicos, ésta no se debería incluir bajo ninguna circunstancia en el cuerpo del mensaje, sino en un archivo individual protegido por contraseña/cifrado, la contraseña no debe estar contenida en el cuerpo del mensaje del que se envía la información, sino en un mensaje distinto o comunicarse por otro medio (por ejemplo, por teléfono). Cuando se recibe información en un mensaje electrónico, sin importar quien lo haya enviado, se debe ser cuidadoso con los archivos y ligas adjuntas cuando éstas no son esperadas, por ejemplo, un mensaje de un proveedor que pide revisar una cotización no solicitada abriendo un archivo adjunto o dando *clic* a una liga específica. En tal caso hay que verificar, (por ejemplo, por teléfono) con el remitente del mensaje y/o utilizar herramientas antimalware para verificar el contenido.

Importante: El Análisis de Brecha

Un análisis de brecha es una comparación de las medidas de seguridad existentes en una empresa u organización contra las que sería conveniente tener, a fin de establecer un plan de trabajo para completar las medidas de seguridad faltantes.

Casos de la vida real: Dr. Pérez, realizando un Análisis de Brecha de las medidas de seguridad

Para responder las preguntas planteadas en la Etapa 2 el Dr. Pérez llenó una tabla como la que se muestra a continuación:

Análisis de Brecha del Dr. Pérez (Medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
A.	Medidas de seguridad basadas en la cultura del personal			

A.1.	*¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?*	X		Parcialmente
A.1.1.	Política de escritorio limpio		X	
A.1.2.	Hábitos de cierre y resguardo	X		
A.1.3.	Impresoras, escáneres, copiadoras y buzones limpios		X	
A.1.4.	Gestión de bitácoras, usuarios y acceso		X	
A.2.	*¿Tienes mecanismos para eliminar de manera segura la información?*		X	
A.2.1.	Destrucción segura de documentos		X	
A.2.2.	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico		X	
A.2.3.	Fijar periodos de retención y destrucción de información		X	
A.2.4.	Tomar precauciones con los procedimientos de re-utilización		X	
A.3.	*¿Has establecido y documentado los compromisos respecto a la protección de datos?*	X		
A.3.1.	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos		X	
A.3.2.	Fomentar la cultura de la seguridad de la información		X	
A.3.3.	Difundir noticias en temas de seguridad		X	
A.3.4.	Prevenir al personal sobre la *Ingeniería Social*		X	
A.3.5.	Asegurar la protección de datos personales en subcontrataciones	X		
A.4.	*¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?*		X	
A.4.1.	Tener un procedimiento de notificación		X	
A.4.2.	Realizar revisiones y auditorías		X	
A.5.	*¿Realizas respaldos periódicos de los datos personales?*		X	
B.	Medidas de seguridad en el entorno de trabajo físico			
B.1.	*¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?*	X		
B.1.1.	Alerta del entorno de trabajo	X		
B.1.2.	Mantener registros del personal con acceso al entorno de trabajo	X		
B.2.	*¿Tienes medidas de seguridad para evitar el robo?*	X		
B.2.1.	Cerraduras y candados	X		
B.2.2.	Elementos disuasorios	X		
B.2.3.	Minimizar el riesgo oportunista		X	
B.3.	*¿Cuidas el movimiento de información en entornos de trabajo físicos?*	X		
B.3.1.	Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico		X	Salvo el celular del Dr. Pérez, ningún otro elemento para tratar

				datos personales sale de su consultorio.
B.3.2.	Mantener en movimiento sólo copias de la información, no el elemento original	X		
B.3.3.	Usar mensajería certificada	X		
C.	Medidas de seguridad en el entorno de trabajo digital			
C.1.	*¿Realizas actualizaciones al equipo de cómputo?*	X		
C.2.	*¿Revisas periódicamente el software instalado en el equipo de cómputo?*		X	
C.3.	*¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?*	X		
C.3.1.	Uso de contraseñas y/o cifrado	X		
C.3.2.	Uso de contraseñas solidas		X	
C.3.3.	Bloqueo y cierre de sesiones	X		
C.3.4.	Administrar usuarios y accesos	X		
C.4.	*¿Revisas la configuración de seguridad del equipo de cómputo?*		X	
C.5.	*¿Tienes medidas de seguridad para navegar en entornos digitales?*	X		
C.5.1.	Instalar herramientas antimalware y de filtrado de tráfico	X		
C.5.2.	Reglas de navegación segura		X	
C.5.3.	Reglas para la divulgación de información		X	
C.5.4.	Uso de conexiones seguras		X	
C.6.	*¿Cuidas el movimiento de información en entornos de trabajo digitales?*	X		
C.6.1.	Validación del destinatario de una comunicación	X		
C.6.2.	Seguridad de la información enviada y recibida		X	

Después de contestar las preguntas respecto a sus medidas de seguridad el Dr. Pérez podrá elaborar su plan de trabajo con un objetivo muy claro: responder que "Sí" a todas las medidas de seguridad que aplican a su tratamiento de datos personales.

En el **Anexo B** se proporciona una tabla en blanco similar a la del Dr. Pérez para que las organizaciones elaboren su propio análisis de brecha.

Resumen de la Etapa 2

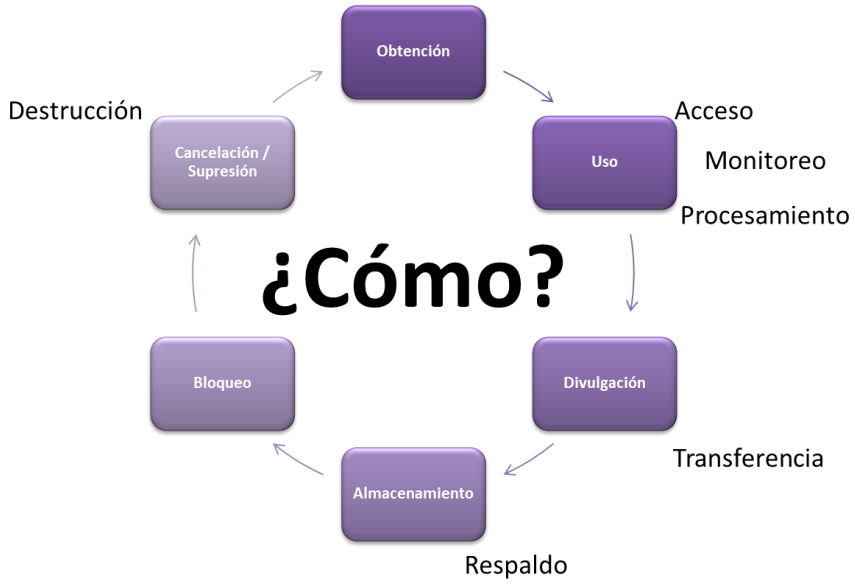
¿Qué ha hecho el Dr. Pérez hasta este momento?

En esta etapa, el Dr. Pérez logró identificar y documentar:

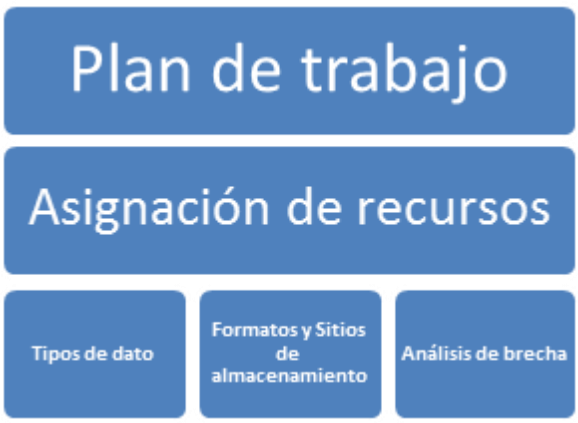
- ☑ Las medidas de seguridad con las que ya cuenta, así como las que requerirá incluir en su plan de trabajo.

Etapa 3. Plan de trabajo

Al llegar a esta etapa los responsables ya han adquirido una noción general del ciclo de vida de los datos personales bajo su custodia, principalmente si están controlando la armonía de dicho ciclo: obtención, uso, comunicación de los datos a terceros (divulgación, transferencia o remisión), si se respaldan, su bloqueo y finalmente su destrucción segura.



También se tienen identificados los tipos de datos, los formatos, los medios de almacenamiento y los sitios de resguardo, así como una relación de las medidas de seguridad existentes y faltantes**. Es decir, se tienen todos los elementos para decidir las acciones prioritarias para proteger los datos personales.**



El plan de trabajo debe reflejar los recursos disponibles, humanos, económicos, de conocimiento y de tiempo con los que se cuenta. En ese sentido, un plan de trabajo debe contener al menos:

- La selección de las acciones prioritarias.
- El periodo en el que se pretende cumplir esas acciones.
- Los recursos humanos y materiales para el cumplimiento de las acciones.
- Las acciones que quedan fuera para el plan de trabajo actual y que se considerarán en el plan de trabajo siguiente.

Las MIPYMES y pequeñas organizaciones tienen que ponderar sus prioridades en función de sus posibilidades económicas y oportunidades de negocio, si es necesario contratar ayuda de un especialista o si dedicarán tiempo a estudiar y aplicar ellos mismos los controles. Salvo algunos controles como las revisiones y auditorías, los responsables de microempresas y pequeñas organizaciones pueden optar por aumentar su nivel de seguridad ellos mismos, **los controles propuestos en este manual están enfocados en la menor inversión monetaria a cambio de que se fomente la cultura de la protección de datos.**

Casos de la vida real: Plan de trabajo del Dr. Pérez

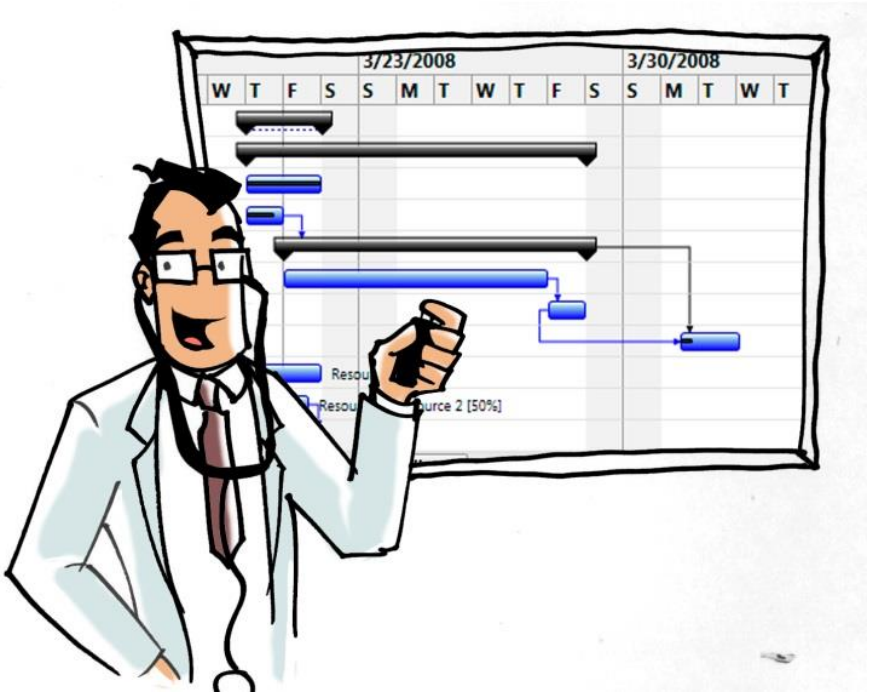
El Dr. Pérez realiza un listado de todas las **medidas de seguridad faltantes** de acuerdo a su análisis de brecha. Considerando sus medios y sitios de resguardo, decide atender primero todas las **medidas de seguridad** que involucran el **entorno de trabajo digital**.

Código	Pregunta o Control
A.	Medidas de seguridad basadas en la cultura del personal
A.1.1.	Política de escritorio limpio
A.1.3.	Impresoras, escáneres, copiadoras y buzones limpios
A.1.4.	Gestión de bitácoras, usuarios y acceso
A.2.1.	Destrucción segura de documentos
A.2.2.	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico
A.2.3.	Fijar periodos de retención y destrucción de información
A.2.4.	Tomar precauciones con los procedimientos de re-utilización
A.3.1.	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos
A.3.2.	Fomentar la cultura de la seguridad de la información
A.3.3.	Difundir noticias en temas de seguridad

A.3.4.	Prevenir al personal sobre la *Ingeniería Social*
A.4.	*¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?*
A.4.1.	Tener un procedimiento de notificación
A.4.2.	Realizar revisiones y auditorías
A.5.	*¿Realizas respaldos periódicos de los datos personales?*
B.	Medidas de seguridad en el entorno de trabajo físico
B.2.3.	Minimizar el riesgo oportunista
C.	Medidas de seguridad en el entorno de trabajo digital
C.2.	*¿Revisas periódicamente el software instalado en el equipo de cómputo?*
C.3.2.	Uso de contraseñas solidas
C.4.	*¿Revisas la configuración de seguridad del equipo de cómputo?*
C.5.2.	Reglas de navegación segura
C.5.3.	Reglas para la divulgación de información
C.5.4.	Uso de conexiones seguras
C.6.2.	Seguridad de la información enviada y recibida

El Dr. Pérez se ha comprometido a tener esas siete medidas de seguridad en un periodo de seis meses, para ello ha solicitado ayuda a su sobrino que estudia ingeniería en sistemas y también se ha comprometido a estudiar una hora diaria la configuración de seguridad de su equipo de cómputo, para después ayudar y explicar a su asistente las medidas de seguridad que se están poniendo en marcha.

La decisión del Dr. Pérez sobre qué controles implementar primero no fue a la ligera, entiende que implementar medidas de seguridad es un proceso que requiere dedicación, y que en su caso, por tratar datos sensibles, tiene que ser especialmente analítico. El entendimiento de su ciclo de tratamiento de datos personales lo ha hecho consiente de que la cantidad de información en sus equipos de cómputo lo obligan a atenderlos prioritariamente sobre otras consideraciones. **Una vez concluido el periodo de seis meses el Dr. Pérez evaluará sus avances y se planteará nuevos controles hasta cumplir con su lista de pendientes.**



Resumen de la Etapa 3

¿Qué ha hecho el Dr. Pérez hasta este momento?

El Dr. Pérez en esta etapa logró:

- ☑ Poner en marcha un plan de trabajo: designar recursos para programar ciclos y tiempos de cumplimiento.

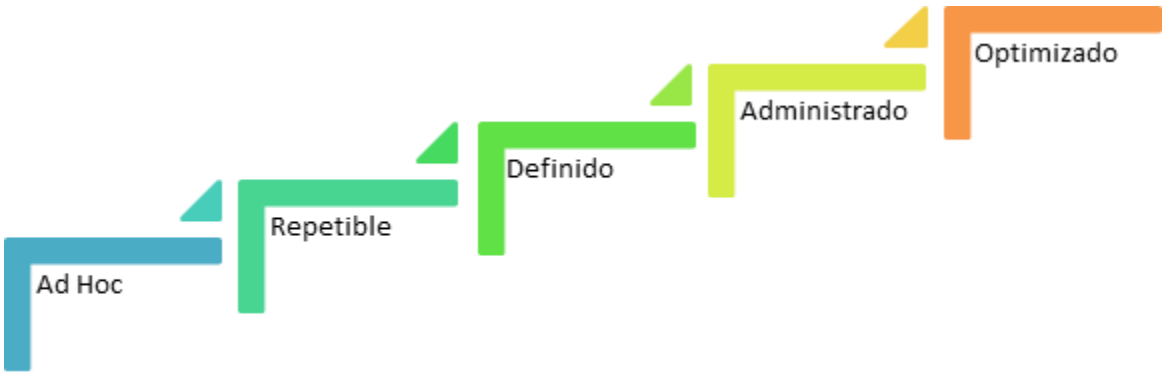
Etapa 4. Mejora continua

Una vez que las empresas y organizaciones han logrado establecer todos los controles de seguridad básicos, es decir, **a través de su plan de trabajo de la Etapa 3 han logrado implementar todas las acciones y medidas de seguridad planteadas en la Etapa 2**, entonces pueden empezar a mejorar periódicamente sus controles a través de un modelo de madurez.

Importante: El valor de documentar las acciones para la seguridad

Uno de los principales obstáculos para el desarrollo de la seguridad en organizaciones de cualquier tamaño es la falta de documentación. Las MIPYMES pueden empezar teniendo por documentación formatos como los que ofrece este manual, sin embargo, conforme progresen a través del modelo de madurez, se puede tener mejor documentación que pueda ser utilizada por ejemplo, para demostrar el tratamiento legítimo de la información ante los titulares o las autoridades, **así como tener mejores estrategias y soporte documental ante una vulneración a la seguridad de los datos personales.**

El modelo de madurez es una escalera donde se pueden considerar cinco niveles:



- **Ad Hoc:** Cada control de la Etapa 2 muy posiblemente empiece aquí, se pasó de no tener nada a tener una implementación dinámica, reactiva y con poca documentación.
- **Repetible:** Existe reglas claras sobre el control de seguridad, se pueden identificar resultados aunque la disciplina todavía es poca.

- **Definido:** El control tiene un conjunto de reglas definidas y bien documentadas tanto en proceso como en personal involucrado.
- **Administrado:** El control posee indicadores y mecanismos que permiten monitorearlo y realizar actualizaciones afectando de manera mínima los procesos de la organización.
- **Optimizado:** El control se enfoca en mejorar su despeño a través de mejores prácticas y las innovaciones tecnológicas que van surgiendo.

Existen circunstancias especiales en las que una organización tendría que evaluar su posibilidad de aumentar su nivel y madurez en uno o más controles:

- Cuando haya crecimiento o una nueva oportunidad de negocio para la organización.
- Como resultado de la revisión o auditoría de un tercero.
- Debido a la ocurrencia de una vulneración a la seguridad de la información.

Si debido a una falta de recursos económicos o materiales la organización no puede emprender un proceso de mejora periódica, al menos debería revisar de manera anual que sus medidas de seguridad se mantengan al día y que no se encuentren disminuidas ante el avance tecnológico o el cambio de las leyes.

Casos de la vida real: La mejora continua de las medidas de seguridad del Dr. Pérez

Después de un año, el Dr. Pérez ha logrado con su plan de trabajo implementar todos los controles de la Etapa 2, es decir, su nivel de madurez sería Ad Hoc, pues es la primera vez que de manera ordenada y secuencial se acerca al tema de seguridad de la información.

Para progresar en el nivel de sus controles a un **nivel Repetible, el Dr. Pérez se dedicará a que las reglas y procedimientos que se han establecido se conviertan en reglas muy claras** y se empiece a tener disciplina en el cumplimiento de los mismas.

Cuando el Dr. Pérez y su asistente atiendan de manera automática las reglas y procesos, el control habrá llegado a un nivel Definido, de forma tal que si el negocio crece, a los nuevos integrantes podrán unirlos rápidamente a la cultura de la seguridad del consultorio.

Conforme el crecimiento del negocio y su conocimiento lo permita, el Dr. Pérez invertirá en tecnología para alcanzar los niveles de Administrado y Optimizado.

De manera independiente a estas predicciones y objetivos, **el Dr. Pérez revisará al menos una vez al año, ya sea por su cuenta o con la asesoría de un tercero, que su nivel de madurez no disminuya.**

Resumen de la Etapa 4

¿Qué ha hecho el Dr. Pérez hasta este momento?

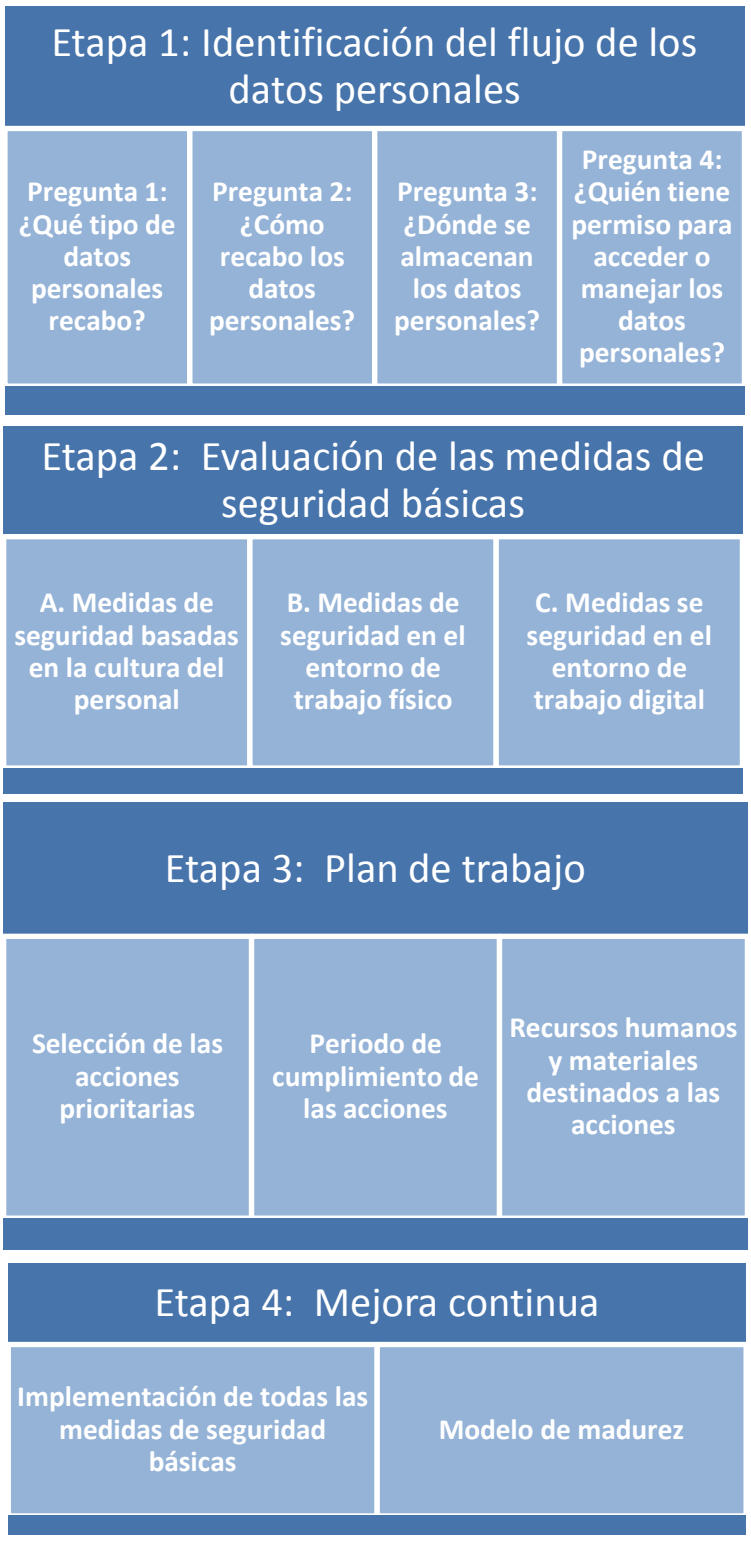
En esta etapa el Dr. Pérez logró:

- ☑ Comprometerse de manera periódica a revisar que su nivel de madurez en el tema de seguridad no disminuya, y en la medida de lo posible aumentarlo.

“La seguridad no es proyecto, es un esfuerzo constante”

Mapa de ruta de las acciones para la seguridad

A continuación se muestra un diagrama con las acciones que contempla el Manual para la implementación de medidas de seguridad en la organización.



ANEXOS

Anexo A. Inventario de datos personales

A.1 Tabla de identificación de tipos de datos personales

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre			
Estado Civil			
Registro Federal de Contribuyentes (RFC)			
Clave Única de Registro de Población (CURP)			
Lugar de nacimiento			
Fecha de nacimiento			
Nacionalidad			
Domicilio			
Teléfono particular			
Teléfono celular			
Correo electrónico			
Nombre de usuario en redes sociales			
Firma autógrafa			
Firma electrónica			
Edad			
Fotografía			
Referencias personales			
Datos sobre características físicas			
Color de piel			
Color de iris			

Datos personales recabados	Existente	Necesario	No necesario
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen del iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña			
Domicilio de trabajo			
Correo electrónico institucional			
Teléfono institucional			
Referencias laborales			
Información generada durante los procedimientos de reclutamiento, selección y contratación			
Experiencia/Capacitación laboral			
Datos académicos			
Trayectoria educativa			
Títulos			
Cédula profesional			
Certificados			
Reconocimientos			

Datos personales recabados	Existente	Necesario	No necesario
Datos migratorios			
Entrada al país			
Salida del país			
Tiempo de permanencia en el país			
Calidad migratoria			
Derechos de residencia			
Aseguramiento			
Repatriación			
Datos patrimoniales y/o financieros			
Bienes muebles			
Bienes inmuebles			
Información fiscal			
Historial crediticio/Buró de crédito			
Ingresos			
Egresos			
Cuentas bancarias			
Números de tarjetas de crédito			
Información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin)			
Seguros			
Afores			
Datos sobre pasatiempos, entretenimiento y diversión			
Pasatiempos			
Aficiones			

Datos personales recabados	Existente	Necesario	No necesario
Deportes que practica			
Juegos de su interés			
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			
Otros datos personales			
Datos personales sensibles			
Datos sobre la ideología			
Posturas religiosas/ ideológicas/morales/ filosóficas			
Pertenencia a un partido/Posturas políticas			
Pertenencia a un sindicato			
Datos de salud			
Estado de salud físico presente, pasado o futuro			
Estado de salud mental presente, pasado o futuro			
Información genética			
Datos sobre vida sexual			
Preferencias sexuales			
Prácticas o hábitos sexuales			
Datos de origen étnico o racial			
Pertenencia a un pueblo, etnia o región			
Otros datos personales sensibles			

A.2 Tabla de identificación de los formatos de almacenamiento de datos personales y esquema de privilegios

Formato de almacenamiento	Físico	Electrónico	¿Quiénes tienen privilegios de uso?
Correspondencia/Correo			
Formularios			
Copias de documentos de identificación			
Solicitudes de pedido			
Facturas			
Bases de datos			
Hojas de cálculo			
Contratos			
Expedientes			
Audio y/o Video			
Otros			

A.3 Tabla de identificación de sitios y medios de almacenamiento de datos personales y esquema de privilegios

Sitios de resguardo	**¿Qué medios de almacenamiento se resguardan?**	**¿Quiénes tiene privilegios de acceso?**
Oficinas de la empresa		
Oficina en casa		
Instalaciones de terceros		
Otros		
Medios de almacenamiento físico	**¿Qué formatos o medios de almacenamiento se resguardan?**	**¿Quiénes tiene privilegios de acceso?**
Escritorios/Cajones		
Estantes/Archiveros		
Bóvedas/cajas fuertes/cuartos de seguridad		
Carpetas/Organizadores		
Otros		
Medios de almacenamiento electrónico	**¿Qué formatos de almacenamiento electrónico se resguardan?**	**¿Quiénes tiene privilegios de uso?**
Computadoras de escritorio		
Computadoras portátiles (Laptop)		
Servidores propios		
Teléfonos inteligentes, tabletas y otros dispositivos móviles		
Memorias USB, discos duros extraíbles y otros medios de almacenamiento electrónico		
CD, DVD,Blue Ray		
Almacenamiento en línea/Cómputo en la nube		
Otros		

Anexo B. Análisis de brecha

Análisis de Brecha (Medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
A.	Medidas de seguridad basadas en la cultura del personal			
A.1.	*¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?*			
A.1.1.	Política de escritorio limpio			
A.1.2.	Hábitos de cierre y resguardo			
A.1.3.	Impresoras, escáneres, copiadoras y buzones limpios			
A.1.4.	Gestión de bitácoras, usuarios y acceso			
A.2.	*¿Tienes mecanismos para eliminar de manera segura la información?*			
A.2.1.	Destrucción segura de documentos			
A.2.2.	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico			
A.2.3.	Fijar periodos de retención y destrucción de información			
A.2.4.	Tomar precauciones con los procedimientos de re-utilización			
A.3.	*¿Has establecido y documentado los compromisos respecto a la protección de datos?*			
A.3.1.	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos			
A.3.2.	Fomentar la cultura de la seguridad de la información			
A.3.3.	Difundir noticias en temas de seguridad			
A.3.4.	Prevenir al personal sobre la *Ingeniería Social*			
A.3.5.	Asegurar la protección de datos personales en subcontrataciones			
A.4.	*¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?*			
A.4.1.	Tener un procedimiento de notificación			
A.4.2.	Realizar revisiones y auditorías			
A.5.	*¿Realizas respaldos periódicos de los datos personales?*			
B.	Medidas de seguridad en el entorno de trabajo físico			
B.1.	*¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?*			
B.1.1.	Alerta del entorno de trabajo			
B.1.2.	Mantener registros del personal con acceso al entorno de trabajo			
B.2.	*¿Tienes medidas de seguridad para evitar el robo?*			
B.2.1.	Cerraduras y candados			
B.2.2.	Elementos disuasorios			
B.2.3.	Minimizar el riesgo oportunista			

Análisis de Brecha *(Medidas de seguridad existentes VS medidas de seguridad faltantes)*				
Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
B.3.	*¿Cuidas el movimiento de información en entornos de trabajo físicos?*			
B.3.1.	Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico			
B.3.2.	Mantener en movimiento sólo copias de la información, no el elemento original			
B.3.3.	Usar mensajería certificada			
C.	Medidas de seguridad en el entorno de trabajo digital			
C.1.	*¿Realizas actualizaciones al equipo de cómputo?*			
C.2.	*¿Revisas periódicamente el software instalado en el equipo de cómputo?*			
C.3.	*¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?*			
C.3.1.	Uso de contraseñas y/o cifrado			
C.3.2.	Uso de contraseñas solidas			
C.3.3.	Bloqueo y cierre de sesiones			
C.3.4.	Administrar usuarios y accesos			
C.4.	*¿Revisas la configuración de seguridad del equipo de cómputo?*			
C.5.	*¿Tienes medidas de seguridad para navegar en entornos digitales?*			
C.5.1.	Instalar herramientas antimalware y de filtrado de tráfico			
C.5.2.	Reglas de navegación segura			
C.5.3.	Reglas para la divulgación de información			
C.5.4.	Uso de conexiones seguras			
C.6.	*¿Cuidas el movimiento de información en entornos de trabajo digitales?*			
C.6.1.	Validación del destinatario de una comunicación			
C.6.2.	Seguridad de la información enviada y recibida			

Anexo C. Ejemplos de vulneraciones a la seguridad: Casos de la vida real

A continuación se presentan distintos escenarios de vulneraciones y el aprendizaje que se deriva de ellos. Estos ejemplos pueden ser usados para la capacitación y concientización del personal, y pueden servir de orientación para identificar situaciones que propicien incidentes de seguridad.

Caso 1. Vendedores de seguros

Un agente de seguros solicita a sus clientes y prospectos que le faciliten los datos de contacto de otras personas que pudieran estar interesadas en el producto o servicio que manejan. No existe un control que impida al vendedor hacer posterior uso de los registros recabados una vez que dejó a la empresa.

Aprendizaje

- El vendedor de seguros no debería utilizar los contactos que recabó durante su estancia en una compañía cuando pasa a formar parte de una nueva.
- Las empresas de seguros deben cuidar que sus empleados o los agentes que trabajan a su nombre obtengan los datos personales cumpliendo con el principio de licitud, información y consentimiento.

Caso 2. Intercambio de bases de datos

El personal de ventas de servicios, seguros, tiempos compartidos, autos, etc. además de solicitar referidos a sus clientes y prospectos, ha buscado comprar o intercambiar bases de datos entre sus similares de otras áreas, para así identificar clientes alineados a ciertos perfiles de ingresos, puesto, hábitos, zona geográfica, etc. Esto pareciera no tener una afectación a la empresa, sin embargo se está haciendo una trasferencia de datos personales sin el consentimiento del titular y para fines muy distintos para los que fueron recabados los datos.

Aprendizaje

- El personal sólo debe tener acceso a los datos según el esquema de privilegios establecido.
- Debe evitarse la copia de bases de datos de forma parcial o total en medios de almacenamiento electrónico (como memorias USB o discos externos) a menos que se cuente con la autorización necesaria.
- Deben mantenerse registros que permitan identificar quién realizó copias de la base de datos o exportó parte de ella.

Caso 3. Empleados de una clínica vendiendo información sensible

Un empleado de un hospital es contactado por una empresa farmacéutica para obtener los datos de ciertos pacientes enfermos del mismo padecimiento. El valor de los datos para la farmacéutica es alto y el empleado no ve mayor riesgo en compartirlos y así tener un ingreso extra.

El empleado no notifica de esta situación a nadie del hospital ni a los titulares (pacientes del hospital) de los datos personales sensibles (recordar que los datos de salud son considerados sensibles por la Ley).

Semanas después la farmacéutica publica un reporte en el que notifica que derivado de las investigaciones realizadas ofrecerá a los pacientes de dicho hospital un plan de medicamentos. La farmacéutica contacta directamente a los pacientes y uno de ellos realiza la típica pregunta "¿Cómo obtuvieron mis datos?", a lo cual la farmacéutica le comenta al paciente que esos datos fueron obtenidos de su hospital.

El paciente interpone una denuncia ante el INAI por mal uso de sus datos, en contra del hospital y de la farmacéutica.

Al iniciar las investigaciones el Instituto descubre que ni el hospital ni la farmacéutica, tienen políticas y programas de privacidad al interior de sus organizaciones, que no se ha capacitado al personal y que tampoco existen controles de seguridad para evitar este tipo de situaciones.

Como consecuencia de lo anterior el Instituto impone una multa tanto al hospital como a la farmacéutica, y lo realiza de forma pública, afectándose el prestigio de ambas empresas.

Aprendizaje

- Definir una política de uso de los datos, establecer y aplicar un procedimiento disciplinario en caso de incumplimiento.
- Limitar el acceso a las bases de datos sensibles.
- Registrar qué personal accede a las bases de datos y genera copias o respaldos, estableciendo un procedimiento de autorización para este efecto.

Caso 4. Una secretaria que pierde un documento en un lugar público

La asistente del Director General de una empresa de *Head hunting* (reclutamiento de personal), está trabajando en conseguir los perfiles de varios ejecutivos para una búsqueda que su jefe le delegó.

La asistente en busca de ser proactiva toma los currículos de varios candidatos y se los lleva a casa para hacer marcas y señalizaciones para que su jefe pueda realizar una mejor selección.

Desgraciadamente esa tarde al salir del trabajo, la señorita olvida en el camión el folder donde lleva los expedientes de los ejecutivos en cuestión, importante mencionar que la asistente para evitar una sanción mayor, no notifica dicho accidente. El expediente es encontrado por una persona que se dedica a la venta de servicios financieros (inversiones, afores, etc.), al darse cuenta de que el perfil de dichas personas es muy alto, los contacta inmediatamente para ofrecerle sus servicios.

Uno de los contactados, muy molesto por la situación inquiere al vendedor, sobre la fuente de los datos, a lo cual no contesta, por lo que el ejecutivo asiste al INAI y presenta una denuncia sobre el caso.

Al realizar la investigación, el INAI descubre que los datos salieron de la empresa de *Head Hunting* e inicia una investigación sobre dicha empresa dándose cuenta que no tienen las medidas de seguridad para evitar la fuga de información y que además no notificaron a los titulares dicha vulneración a la seguridad.

Aprendizaje

- Capacitar al personal sobre el tema de datos personales, las regulaciones y las actividades a realizar en el caso de una vulneración a la seguridad.
- Implementar procedimientos a realizar en caso de vulneraciones.
- Registrar los medios de almacenamiento físico y electrónico, y restringir la salida de datos personales.

Caso 5. Descuentos por proporcionar bases de datos

Un empleado, gerente de una empresa, está en el proceso de compra de un automóvil, en dicho proceso, el vendedor le ofrece un descuento si éste le entrega el directorio de la empresa, con el fin de venderles autos.

El comprador ve una oportunidad de obtener un descuento y no ve ningún riesgo mayor en entregar esta lista. Se realiza la venta del auto contra entrega de la lista del directorio de la empresa donde trabaja el comprador.

El vendedor de autos contacta a todos los directivos de la empresa y varios de ellos se molestan por ser contactados, uno de ellos lleva el caso ante el INAI e inician las investigaciones dando como consecuencia que se den 2 casos, tanto el de la empresa del comprador del auto como contra la agencia automotriz, ambas reciben penalizaciones por el mal uso de los datos personales, la falta de capacitación de sus empleados, la falta de controles de seguridad y políticas y programas claros en busca de implantar una cultura de privacidad.

Aprendizaje

- Concientizar al personal sobre la existencia de estas prácticas y su ilegalidad.
- Restringir la exportación de base de datos.
- Restringir los medios de almacenamiento electrónico al personal que no los requiera.
- Establecer e implementar un procedimiento disciplinario en caso de incumplimiento.

Caso 6. El call center

Un empleado de un call center donde se realizan cobros con tarjetas de crédito solicita a los clientes los datos completos de la tarjeta: Nombre del titular, dirección, dígitos de la tarjeta, fecha de vencimiento y código de seguridad CVV2. Con estos datos una persona mal intencionada podría hacer cargos sin la autorización del titular. El empleado copia en una hoja de papel los datos de dos tarjetas al día y realiza compras por internet sin la autorización del titular.

Aprendizaje

- No permitir que los empleados con acceso a este tipo de información tengan acceso a dispositivos donde puedan capturar los datos (físicos o electrónicos).
- Grabar las llamadas, previo consentimiento del cliente.
- Establecer e implementar un procedimiento disciplinario en caso de incumplimiento.