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

Av. Insurgentes Sur núm. 3211, Col. Insurgentes Cuicuilco, C.P. 04530

Del. Coyoacán, México, CDMX.

Primera Edición, diciembre de 2017

Impreso en México / Printed in Mexico

Distribución gratuita

Temario

Introducción

El INAI ha desarrollado este manual, que permitirá al lector conocer los objetivos y alcances en materia de medidas de seguridad para la protección de los datos personales en posesión de los particulares, con el propósito de brindar información y orientarle en el cumplimiento de sus obligaciones en materia de seguridad de los datos personales.

¡Esperamos que su experiencia resulte positiva!

Objetivo general

Al concluir el presente manual, usted distinguirá las medidas de seguridad, su relevancia, las obligaciones y responsabilidades plasmadas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, con el propósito de implementar un Sistema de Gestión de Seguridad de Datos Personales para la protección de los datos personales en su entorno de trabajo.

Elementos del manual

A lo largo del manual revisará los contenidos de tres módulos con los temas centrales, que se presentan organizados didácticamente, utilizando la metodología del aprendizaje basado en problemas, además de los recursos que le servirán de apoyo para su mejor comprensión.

Luego de concluir cada uno de los módulos encontrará la evaluación de aprendizaje, la cual, le ayudará a verificar su nivel de conocimientos y el logro de los objetivos alcanzados.

Asimismo, se muestran diversos recuadros denominados, **recuerde**, o **referencias normativas** destacadas, que aunado a la realización de los **ejercicios de reflexión o de trabajo**, le permitirán reforzar sus conocimientos.

Se proponen también **lecturas complementarias**, **referencias a materiales adicionales de consulta y material interactivo** para profundizar en los temas.

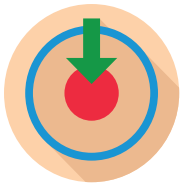
A continuación, se describen los elementos del manual a los que hemos hecho referencia:

1.- Recuerde

En este apartado, se resumen conceptos que debe tener presentes en todo momento, para comprender el contenido que se explica en cada módulo.

2.- Ejercicios de reflexión

En este apartado, se proponen ejercicios que promuevan el análisis de los contenidos, respecto a su propia experiencia.



3.- Ideas clave

En este apartado, encontrará la definción del concepto más importante que se describe en cada párrafo.

4.- Ejercicios de trabajo

El propósito de este apartado es que mediante la realización de ejercicios aplique sus conocimientos y habilidades para que logre los aprendizajes deseados.

5.- Referencia normativa

En este apartado, encontrará referencias a las leyes, reglamentos y otras disposiciones normativas aplicables en materia de protección de datos personales en posesión de los particulares, con el propósito de orientar sus acciones en apego a la Ley.

6.- Material interactivo

En este apartado encontrará material interactivo que podrá consultar a través de su dispositivo. Se recomienda que cuando elija una aplicación para la descarga, verifique lo realtivo a la confidencialidad y la protección de los datos en su dispositivo.


1
Módulo

Módulo 1

Conceptos fundamentales en materia de protección de datos personales en posesión de los particulares y medidas de seguridad.

Objetivo particular:

Al concluir el módulo, identificará las ventajas de implementar las medidas de seguridad para la protección de los datos personales en posesión de los particulares, en su entorno de trabajo.

Evaluación de antecedente

Con el propósito de identificar su nivel de conocimiento respecto al tema de medidas de seguridad, le pedimos revise el siguiente material y responda las preguntas de reflexión que se presentan.

Video: http://www.avpd.euskadi.eus/s04-5248/es/contenidos/informacion/documentos_difusion/es_difusion/luces.html [1]

Ejercicio de reflexión

Instrucciones.
Responda las siguientes preguntas:

1.- ¿Ha vivido alguna situación semejante a la del protagonista de esta historia?

2.- ¿Se ha sentido vulnerado en su privacidad en relación con llamadas insistentes o solicitudes de datos personales vía telefónica, por correo electrónico o en su domicilio, entre otras?

3.- ¿Alguna vez ha presentado una queja por el uso inadecuado de sus datos personales? ¿Ante quién? ¿Le ha dado seguimiento? ¿Recibió la solución adecuada?

4.- ¿En el cumplimiento de sus funciones, ha solicitado datos personales a alguien? ¿Le ha explicado la finalidad de obtenerlos?

[1] El video denominado “Las luces funcionan” es propiedad de la Agencia Vasca de Protección de Datos quien llegó a un acuerdo con la Oficina del Comisionado de la Información del Reino Unido (Information Commissioner´s Office, ICO) para adaptar y editar un video formativo bajo su licencia. El video es una breve introducción dramatizada a los principios de la protección de datos. Se elaboró con fines didácticos y su uso estaba pensado como parte de un programa de sensibilización y formación para los trabajadores que ayude a las organizaciones en el cumplimiento de los requerimientos legales y en la adopción de buenas prácticas. También es un material de difusión válido para la ciudadanía.

Para entender de una manera clara la importancia de la protección a los datos personales, es necesario hacer un ejercicio de reflexión que nos lleve a repensar la relación que tienen los datos con una persona.

Los datos personales son aquellos que permiten que alguien sea identificado o identificable. La protección de los datos es un derecho humano y su reconocimiento ha sido progresivo; mucho tiene que ver el camino que sigue esta progresión con la realidad social, ya que ésta, al igual que el derecho, es dinámica.

Actualmente, gracias a las herramientas tecnológicas con las que contamos es más sencillo recolectar y compartir los datos personales, por lo que nace la necesidad del reconocimiento de este derecho y la implementación de instrumentos jurídicos que garanticen su ejercicio y protección.

Ejercicio de trabajo 1.- Las situaciones clave.

Instrucciones.
A partir de la revisión que hizo del video, vamos a recorrer juntos algunos de sus elementos. Para ello, llene el siguiente cuadro con base en las cuatro situaciones clave que observó en el video.

Identifique y responda a partir de las preguntas planteadas.

Situación	Preguntas	Escriba lo que sucedió en esta situación
La recepcionista del hotel demanda información privada al huésped.	¿Qué fue lo que pasó? ¿Qué errores identificó en la actitud de la recepcionista? ¿Cuáles fueron los errores que cometió el huésped?	
El huésped en su habitación brinda datos personales en respuesta a una llamada telefónica.	¿Qué error cometió el huésped que quebrantó la seguridad de los datos personales que él tenía de sus clientes? ¿En algún momento preguntó la razón por la cuál estaban solicitándole datos personales? ¿Se ha preguntado por qué dio respuesta a todo lo que preguntaban?	

Situación	Preguntas	Escriba lo que sucedió en esta situación
Una mujer llama solicitando datos personales de quien dice ser su esposo.	¿Considera que existe algún problema al brindar datos personales sin una clara identificación de la veracidad de la identidad de la persona que los solicita? ¿Qué efectos puede tener el hecho de haber brindado datos personales a alguien desconocido?	
Una persona solicita a una empresa de ventas eliminar sus datos personales de la base de datos para no recibir más llamadas telefónicas.	¿La persona conocía para qué iban a utilizarse sus datos personales antes de darlos? ¿Qué derecho está reclamando esta persona que desea ser dada de baja del sistema de datos?	

El propósito del ejercicio fue resaltar la relevancia que tienen las medidas de seguridad, tanto al brindar como al solicitar datos personales sin conocer el destino, o la razón por la cual los proporciona o solicita. Para confirmar esta reflexión, revise las medidas de seguridad que establece el Artículo 19 de la LFPDPPP, que a continuación se incluye.

Art.19.-Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Una vez que sabe la importancia del derecho a la protección de los datos personales y la relación que tiene con cada persona, puede imaginar los escenarios negativos, si no hace un adecuado tratamiento. Como se observa, es de suma importancia contribuir a su protección mediante la implementación de medidas de seguridad que disminuyan las amenazas y posibles vulneraciones.

Respetar el derecho de protección a los datos personales disminuye escenarios de riesgo.

Después de describir la importancia de la protección de los datos personales, por favor, lea el siguiente problema:

Una mañana del mes de marzo, el Señor Gregorio Martínez se presentó en la Notaría Pública que queda cerca de su casa; aquella en la que hace un par de meses había iniciado algunos trámites para la venta de su propiedad. En aquel momento la venta no pudo concretarse debido a algunos adeudos.

En los pasados seis meses ha debido cubrirlos a fin de hacer realidad un sueño que hace mucho rondaba su cabeza: vender la única propiedad que había heredado de sus padres. Una casa demasiado grande para él, y cuya venta le permitiría comprar dos propiedades más pequeñas: una para habitarla y la otra para rentarla. El Señor Martínez ya no es un hombre joven y tener una entrada fija, al menos de una renta, era algo que planeaba.

Esta vez se presentó para darle a su abogado la buena nueva de que ya tenía un comprador, a quien había podido convencer de la compra; y quién utilizando todos sus recursos, estaba dispuesto a cerrar el trato cuanto antes. Se trataba, como ya dijimos de una casa heredada, pero cuyos papeles se encontraban en regla y no presentaba ya ningún adeudo, lo que permitiría hacer la venta lo antes posible y quizá para antes de que acabara el año ya podría gozar de los primeros meses de recibir una renta.

El Señor Gregorio Martínez no había hecho cita ese día, pero se presentó puntual a la Notaria y la señorita de la recepción le indicó que el Licenciado Gómez podría atenderlo en media hora. Esperó paciente a que en una de las salas de la Notaría le prestara oído a su buena noticia. En el mes de septiembre había entregado toda su documentación y su expediente personal continuaba bajo el resguardo de la Notaría. Le contó al Licenciado Gómez de su nuevo comprador y de la necesidad de reabrir su trámite lo antes posible, mostró los pagos que se adeudaban el año pasado ya cubiertos, así que todo estaba listo para retomar la operación.

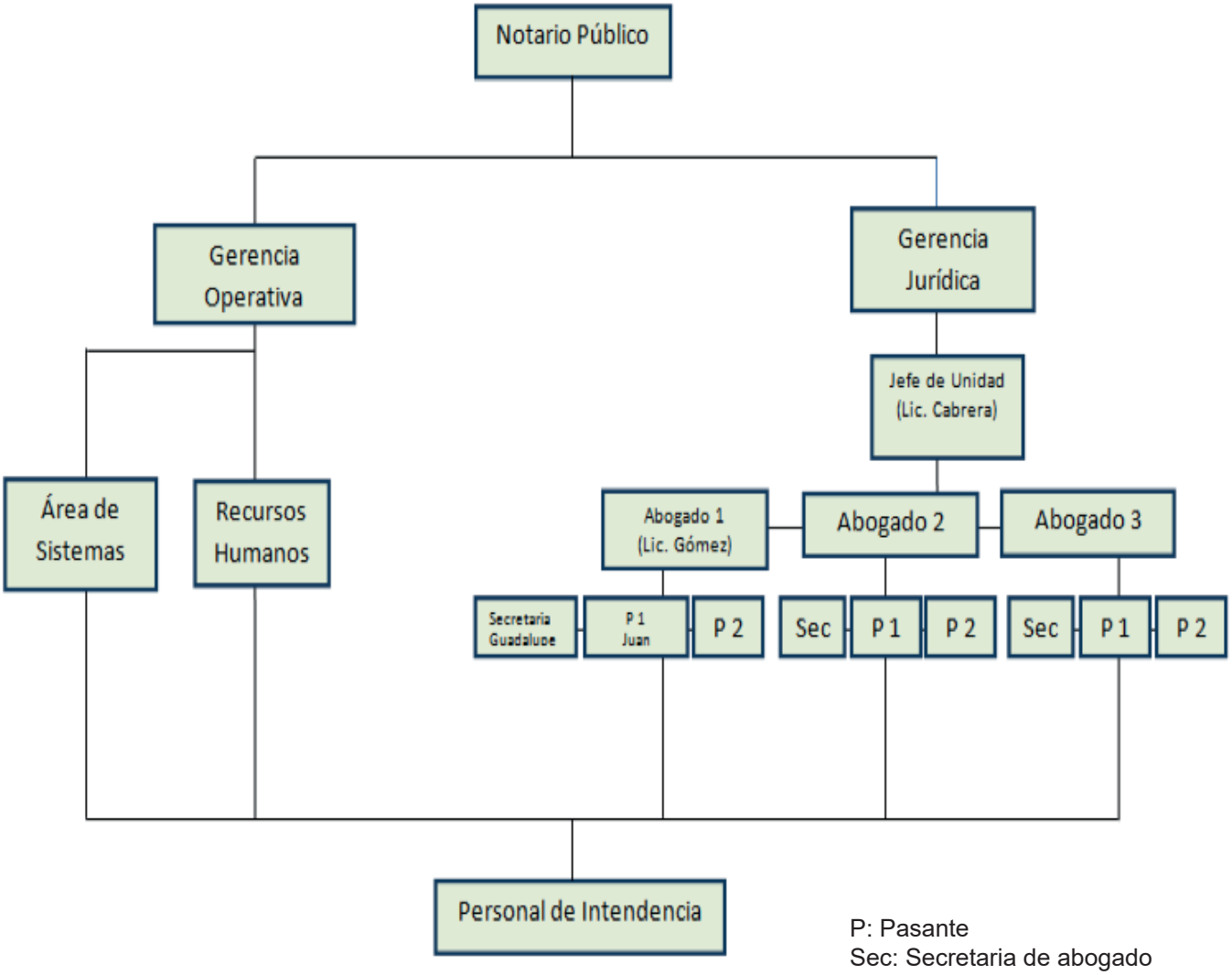
El Licenciado Gómez salió de la sala para traer el expediente del Señor Martínez, pero se llevó una sorpresa mayúscula cuando al llegar a su oficina y comenzar a revisar el estante donde guardaba todos los expedientes, justo ése no estaba. Buscó lo más rápido que pudo y ¡nada!, era como si la Tierra se lo hubiera tragado, le preguntó a Guadalupe, su secretaria, si tenía ese expediente, ella negó con la cabeza y puso cara de preocupación. Después preguntó a los pasantes que tenía a su cargo si alguno de ellos lo había tomado, una negó con la cabeza pues no sabía ni de qué expediente estaba hablando el Licenciado y otro más dijo que él lo había entregado a la secretaria el día de la última reunión de seguimiento.

El mes pasado, el Licenciado Gómez llegó tarde a su trabajo pues una cuestión con la salud de su hijo le había impedido presentarse a tiempo para la reunión de seguimiento. Aquel día la Licenciada Cabrera, Jefa de Unidad, le había solicitado a uno de los pasantes entregarle todos los expedientes del Licenciado Gómez, argumentando que los requería para la reunión. Una vez pasada la reunión, Juan el pasante, se lo devolvió a Guadalupe, la secretaria.

En virtud de que el expediente no estaba, el Licenciado Gómez decidió regresar con su cliente para proponerle una reunión posterior y darle continuidad a su trámite, con ello buscaba ganar tiempo para encontrar la información del Señor Martínez, posteriormente regresó a su oficina muy enfadado y angustiado. Buscó en su computadora los datos de registro de la propiedad de su cliente a fin de encontrar la forma de recuperar los documentos extraviados, la información que encontró fue que la propiedad ya estaba a nombre de otra persona.

Si su dispositivo cuenta con internet, puede reproducir el siguiente video[2], o bien consulte el vínculo electrónico: https://youtu.be/QI3khMNeiT0

[2] INAI [inaimexico]. (2017, Diciembre). Parte 1medidas de seguridad dirigido a sujetos regulados [Archivo de video]. Recuperado de https://youtu.be/QI3khMNeiT0



P: Pasante
Sec: Secretaria de abogado

Ejercicio de trabajo 2.- Organizando mis ideas.

Instrucciones.
A partir de la revisión del problema que acaba de leer, realice una lluvia de ideas.

La lluvia de ideas es una técnica para ordenar información de manera general, puede hacerlo en forma de lista, palabras sueltas, frases, o bien un mapa con las principales ideas.

.....

.....

.....

.....

.....

.....

Después de leer el problema, conteste la siguiente pregunta:

1.- ¿Considera necesario que el Licenciado Gómez cuente con una lista de registro de los expedientes de sus clientes y de los trabajadores de la Notaría que pueden conocer el contenido de tales expedientes? Explique por qué.

.....

.....

.....

.....

.....

.....

Cuando tratamos datos personales, es indispensable conocer algunos artículos de la LFPDPPP, así como algunas figuras definidas en el Artículo 3, como: el encargado, responsable y titular, que en el siguiente cuadro se describen.

El Artículo 3 de la LFPDPPP define las figuras de encargado, responsable y titular de los datos personales.

Artículo 3.- Para los efectos de esta Ley, se entenderá por:
IX. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.
XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.
XVII. Titular: La persona física a quien corresponden los datos personales.

Ahora, revisemos el Artículo 57 del Reglamento de la LFPDPPP para conocer algunas definiciones básicas de los tres tipos de medidas de seguridad que existen:

Artículo 57 del Reglamento de la LFPDPPP.
El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. **Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales.**

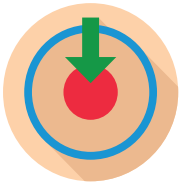
Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad, emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.

Los tipos de medidas de seguridad que existen son:

Administrativas:
• Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.

Físicas:
• Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, para resguardar el entorno y acceso físico a los datos personales.

Técnicas:
•Conjunto de actividades, controles o mecanismos, que se valen de la tecnología para resguardar el entorno digital de los datos personales.



Las **medidas de seguridad administrativas** se entienden como el conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.

Por su parte, las **medidas de seguridad físicas** son el conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:

a. Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;
b. Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;
c. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
d. Garantizar la eliminación de datos de forma segura.

Finalmente, las **medidas de seguridad técnicas** se refieren al conjunto de actividades, controles o mecanismos, que se valen de la tecnología para asegurar que:

a. El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
b. El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c. Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y
d. Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Ahora que sabe lo anterior, seguramente se preguntará ¿por qué debería interesarme la seguridad de los datos personales?

Además de las respuestas que haya encontrado en su reflexión, algunas razones adicionales podrían ser:

- Porque la protección de los datos personales implica el reconocimiento y la protección de un derecho humano.
- Porque eficientar las medidas de seguridad disminuye los riesgos de vulneración a la seguridad de los datos personales.
- Porque proteger los datos personales evita afectaciones económicas debido a multas.
- Porque aumenta la competitividad en una empresa.

Debido a lo anterior, es importante recordar que para una empresa u organización no es posible implementar un programa de seguridad de los datos personales que reduzca el riesgo a cero; sin embargo, se deben poner en marcha medidas de seguridad suficientes para minimizar las vulneraciones a la seguridad de los datos personales y sistemas de tratamiento.

Las categorías anteriores de medidas de seguridad establecidas por la LFPDPPP también se clasifican de la siguiente manera:

Medidas de seguridad basadas en la cultura del personal.

Medidas de seguridad en el entorno de trabajo físico.

Medidas de seguridad en el entorno de trabajo digital.

Cultura del personal

- Hábitos y controles en el acceso a la información.
- Difusión de información y capacitación al personal.
- Eliminación y destrucción segura de información y documentación.
- Procedimientos correctivos ante vulneraciones de seguridad.
- Revisiones y auditorías periódicas.

Entorno físico

- Accesos restringidos salvo personal autorizado.
- Autorización previa a la salida y envío de documentos y/o medios de almacenamiento electrónico.
- Mensajería certificada.
- Cerraduras, candados, alarmas, cámaras y guardias de seguridad.

Entorno digital

- Sistemas operativos, programas y aplicaciones con licencia y actualizaciones periódicas.
- Herramientas antimalware.
- Seguimiento de protocolos para uso de conexiones y navegación seguras.
- Contraseñas sólidas de autenticación para el acceso a información.

Si quiere conocer más sobre estas categorías de medidas de seguridad, revise el Manual en Materia de Seguridad de Datos Personales para MIPYMES y Organizaciones Pequeñas y el Artículo 2 del Reglamento de la LFPDPPP. Puede consultar el manual, en el repositorio del Campus Iniciativa Privada del Centro Virtual de Capacitación en Acceso a la Información y Protección de Datos (CEVINAI): www.inai.org.mx

Hasta el momento y con la información que tiene, conoce la importancia de proteger datos personales, asimismo puede identificar los aspectos fundamentales de un problema en el que se ha vulnerado la seguridad de éstos, por lo que en el módulo 2 revisaremos a profundidad algunas de las obligaciones y responsabilidades establecidas en la LFPDPPP, relativas a las medidas de seguridad, que los sujetos regulados por dicha Ley deben adoptar.

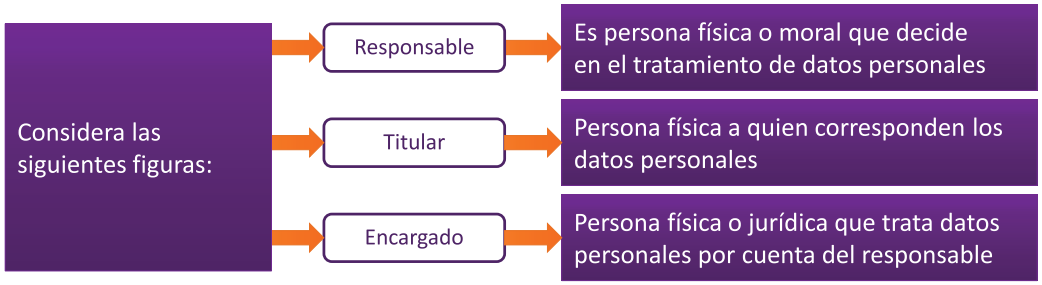
Para concluir el módulo I, le presentamos el siguiente resumen de lo visto hasta este momento:

PROTECCIÓN DE DATOS PERSONALES

La LFPDPPP en su artículo 1 señala que:

Tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legitimo, controlado e informado.

Requiere de medidas de seguridad de tipo:



Evaluación de avance

Instrucciones

A fin de que verifique su nivel de conocimiento, por favor en los espacios en blanco escriba la palabra que complete cada oración.

1. Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad de tipos _____, _____ y _____ que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

2. Es de suma relevancia contribuir a la protección de los datos personales mediante la implementación de medidas de seguridad que disminuyan las _____ y posibles _____ a éstos.

3. El tipo de medidas de seguridad _____ es el conjunto de actividades, controles o mecanismos, que se valen de la tecnología para resguardar el entorno digital de los datos personales.

4. En una empresa u organización, se deben poner en marcha _____ de _____ suficientes para minimizar las vulneraciones a la seguridad de los datos personales y sistemas de tratamiento.

Para validar sus respuestas, consulte en el siguiente vínculo electrónico:


2
Módulo

Módulo 2

Obligaciones y responsabilidades sobre medidas de seguridad de los datos personales en posesión de los particulares.

Objetivo particular

Al concluir el módulo, diferenciará los activos y amenzas a los que están expuestos los datos personales, así como los sitios de resguardo para el almacenamiento de dichos datos en su entorno de trabajo.

Para iniciar con el módulo 2, donde se describen las obligaciones y responsabilidades sobre medidas de seguridad, puede consultar la LFPDPPP y su Reglamento en el repositorio del Campus Iniciativa Privada del CEVINAI:

Los responsables de los datos personales, como ya revisamos en el módulo anterior, no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información, por ejemplo, borrar de manera segura su información, contar con equipos de cómputo con software actualizado y contraseñas seguras, informar al personal sobre sus deberes mínimos de seguridad, entre otras. Asimismo, tomarán en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos personales y el desarrollo tecnológico.

Si quiere conocer más de este tema, revise el Artículo 60 del Reglamento de la LFPDPPP.

Artículo 60 del Reglamento de la LFPDPPP:
El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:

I. El riesgo inherente por tipo de dato personal;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico, y
IV. Las posibles consecuencias de una vulneración para los titulares.

De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:

I. El número de titulares;
II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;
III. El riesgo por el valor potencial cuantitativo y cualitativo que pudiera tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

Si recordamos el problema que presentamos en el módulo 1, el Licenciado Gómez recibió los documentos de un cliente, por lo tanto estaban a su cargo, lo que podemos deducir es que no tomó las precauciones suficientes para el resguardo de la documentación y ello derivó en su extravío.

Hagamos un ejercicio para identificar qué medidas pudo haber instrumentado, para ello, revisemos primero el Reglamento de la LFPDPPP.

Respetar el derecho de protección a los datos personales disminuye escenarios de riesgo.

El Artículo 61 del Reglamento de la Ley establece las siguientes acciones para la seguridad de los datos personales:

Artículo 61.- Si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, éste tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, iniciará el procedimiento a que se refiere este Capítulo, a efecto de determinar la sanción que corresponda.

I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
II. Determinar las funciones y obligaciones de las personas que traten datos personales;
III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;
V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
VII. Llevar a cabo revisiones o auditorías;
VIII. Capacitar al personal que efectúe el tratamiento, y

IX. Realizar un registro de los medios de almacenamiento de los datos personales. El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.

Con estos elementos continuaremos el análisis del problema, por favor, realice el siguiente ejercicio.

Ejercicio de trabajo 3. Lo que el Licenciado Gómez pudo hacer.

Instrucciones.
Elabore una lista de las acciones que el Licenciado Gómez pudo haber realizado para disminuir el riesgo de perder la documentación de su cliente. Además de las medidas indicadas en el Artículo 61 del Reglamento de la LFPDPPP ¿identifica algunas otras?

Acciones

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Otras medidas de seguridad:

A continuación, explicaremos qué es un activo y las amenazas a las que están expuestos. Para comprender esto, es importante que sepa que un activo es cualquier valor para la organización que requiera ser protegido. Hay dos tipos de activos:

TIPOS DE ACTIVOS

Activos de información, corresponden a la esencia de la organización:

- Información relativa a los datos personales.
- Información de procesos del negocio en los que interviene el flujo de datos personales y actividades involucradas en el tratamiento de los mismos.

Activos de apoyo, son aquellos en los cuales residen los activos de información, como son:

- Hardware.
- Software.
- Redes y Telecomunicaciones.
- Personal.
- Estructura organizacional.
- Infraestructura adicional.

Es importante señalar que debe mantenerse actualizado el inventario de activos, así como los medios de almacenamiento en que residen las bases de datos personales.

Ejercicio de reflexión

Recuerde el problema al que se enfrenta el Licenciado Gómez, el personaje principal sobre el que hemos hablado antes. El extravío de los documentos que él tenía devino en una acción deliberada para la venta de la propiedad del Señor Gregorio Martínez.

¿Con qué activos de información del problema que estamos revisando contaba la Notaria?

.....

.....

.....

¿En su empresa u organización, qué activos de información hay?

.....

.....

.....

¿Puede identificar algunas amenazas a la seguridad de los datos personales que posee la Notaría?

.....

.....

.....

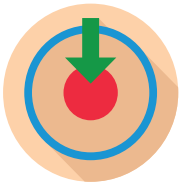
¿Y en su empresa u organización?

.....

.....

.....

Revisemos ahora el tema de las amenazas. Una **amenaza** se refiere a una **circunstancia o evento con la capacidad de causar daño a una organización** y puede ser de origen natural o humano, accidental o deliberada y provenir de adentro o desde afuera de la organización.



Cuando analizamos las vulneraciones a la seguridad de los datos personales es importante tomar en cuenta los distintos tipos de amenazas. Una amenaza tiene el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo, un activo es cualquier valor para la organización que requiera ser protegido.

Los activos deberán ser aquéllos que estén relacionados con el ciclo de vida de los datos personales y sus distintos tratamientos, se deben identificar y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo, es decir, la combinación de la probabilidad de un evento y su consecuencia desfavorable.

Por ejemplo, la pérdida o destrucción no autorizada de los expedientes implica que una persona mal intencionada destruya los archivos físicos o electrónicos que contienen sus expedientes, lo cual impediría otorgarles una adecuada atención a sus clientes.

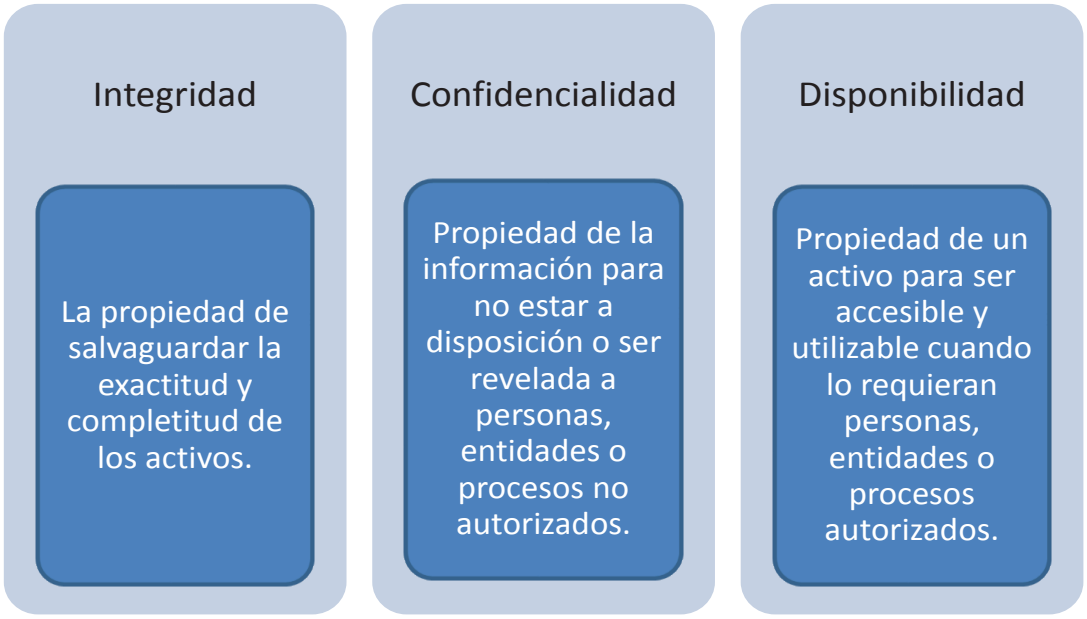
Los activos, como se ha explicado, son la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Los activos son la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Toda esa información que posee su empresa o su organización debe procurar guardarla y difundirla de manera segura. Ahora bien, después de revisar las medidas de seguridad que puede implementar para proteger los datos personales en su entorno de trabajo, es necesario describir qué es la seguridad de la información:

Es la preservación de la integridad, confidencialidad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Vamos a explicar cada uno de estos conceptos:

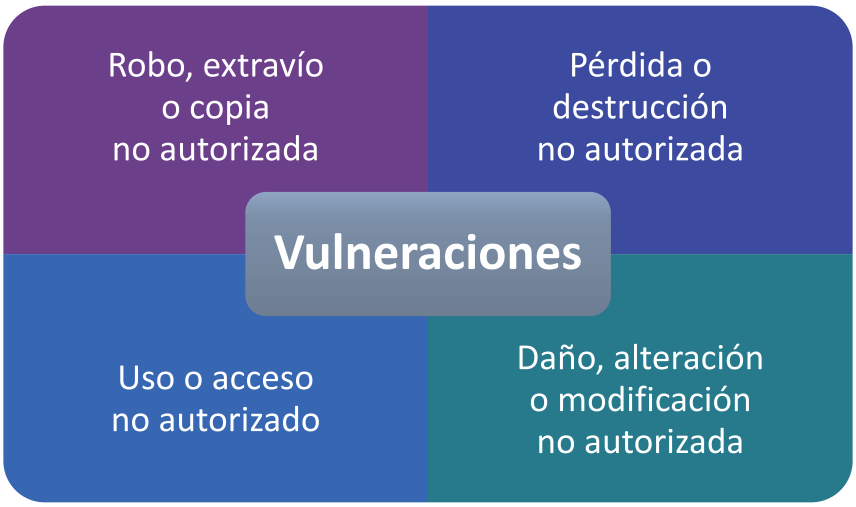


Cualquier sujeto regulado por la LFPDPPP debe tener presentes las medidas de seguridad para disminuir la vulneración de la seguridad de los datos personales, a fin de eficientar su trabajo y darles un tratamiento adecuado a los datos personales en su posesión. Al tener en cuenta de qué forma protegerlos, también evalúa la manera de prevenir vulneraciones a la seguridad. Revisemos el siguiente Artículo de la LFPDPPP que precisa qué se entiende por vulneración:

Artículo 20 de la LFPDPPP:

Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

El artículo de referencia, es de suma importancia para proteger los datos personales y ser consciente de las consecuencias de la vulneración a la seguridad de los datos personales.



Además, es necesario que revise los Artículos 63 a 65 del Reglamento de la LFPDPPP.

Vulneraciones de seguridad.
Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

Notificación de vulneraciones de seguridad.
Artículo 64. 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 las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

Información mínima al titular en caso de vulneraciones de seguridad. Artículo 65. El responsable deberá informar al titular al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde puede obtener más información al respecto.

De la lectura anterior, podríamos imaginar como ejemplo un consultorio médico en el que alguien altere deliberadamente el expediente de algunos pacientes y modifique los padecimientos que presentan, por lo que podría recetar medicamentos y tratamientos inadecuados para cada persona.

También es importante informar al titular cuando ocurra una vulneración, a fin de que éste pueda tomar acciones para reducir el impacto del incidente. En la realidad, pocos responsables llevan a cabo esta acción, ya que suelen verlo únicamente como el reconocimiento de un error y pierden de vista lo benéfico que les resultaría informar en tiempo.

Vuelva al análisis del problema del Licenciado Gómez; en el que uno de sus clientes, ha solicitado continuar con su trámite de compraventa. Al retomar el caso, se da cuenta que el expediente está extraviado, y no sólo eso, la propiedad está a nombre de otra persona.

Ejercicio de reflexión

Instrucciones

Con base en su experiencia, responda las siguientes preguntas:

¿Qué cree que pudo haber sucedido?

¿Cómo pudo una propiedad cambiar de propietario?

¿Considera que algo pudo haber sucedido en la Notaría y que alguien tomó la información para cometer un delito?

¿Esto se pudo haber evitado? Si es así, ¿cómo? Le sugerimos formular algunas ideas sobre el problema.

Después de realizar el ejercicio anterior, con sus respuestas, podrá deducir que el objetivo de implementar medidas de seguridad es que cada una de ellas ayude a reducir el riesgo de que se materialice una vulneración y sus consecuencias desfavorables, lo cual reduce el daño a los titulares y a la empresa u organización.

Ahora bien, otro aspecto relevante en la protección de los datos personales es identificar el ciclo de vida de los datos personales que se muestra en el cuadro de la pagina 73, para facilitarlo, 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.

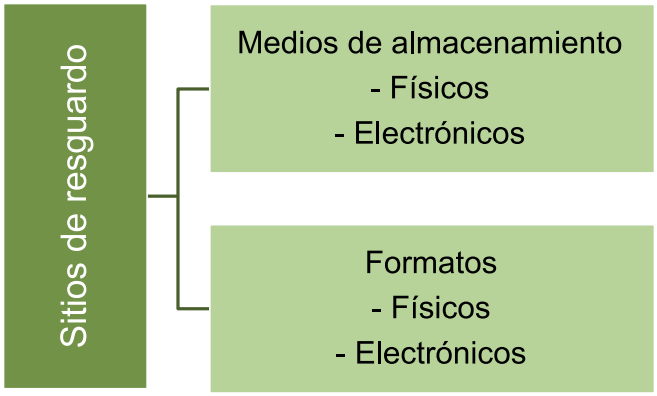
Medio de almacenamiento electrónico: Es todo recurso al que se puede acceder sólo mediante el uso de equipo de cómputo que procese su contenido para examinar, modificar o almacenar los datos personales. Podemos considerar, por ejemplo, discos duros tanto los propios del equipo de cómputo como los portátiles, memorias extraíbles como USB o SD, CDs, Blu-rays, entre otros. También podemos utilizar 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 relativa a datos personales, 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 relativa a datos personales, por ello, a manera de resumen, se presenta el siguiente cuadro:



Con el propósito de que identifique las medidas de seguridad que actualmente aplica en su entorno de trabajo, así como las áreas de oportunidad para mejorar, conteste las siguientes preguntas.

Ejercicio de trabajo 4. En mi contexto laboral.

Instrucciones.

A continuación, le presentamos algunas preguntas a fin de que pueda responderlas pensando en su contexto laboral.

¿En su espacio de trabajo, usted y sus compañeros ponen atención en no dejar a la vista datos personales y llevan registro de su manejo?

.....

.....

.....

¿Lleva un registro o inventario de datos personales? ¿Y de los medios que utiliza para almacenarlos? ¿Cuáles son? Considere las definiciones y el ciclo de vida de los datos personales que acaba de revisar.

.....

.....

.....

¿Cuenta con un análisis de los riesgos existentes a los datos personales que posee en su espacio de trabajo?

.....

.....

.....

.....

¿Sabe qué medidas de seguridad existen para el tratamiento de datos personales en su espacio de trabajo?

.....

.....

.....

.....

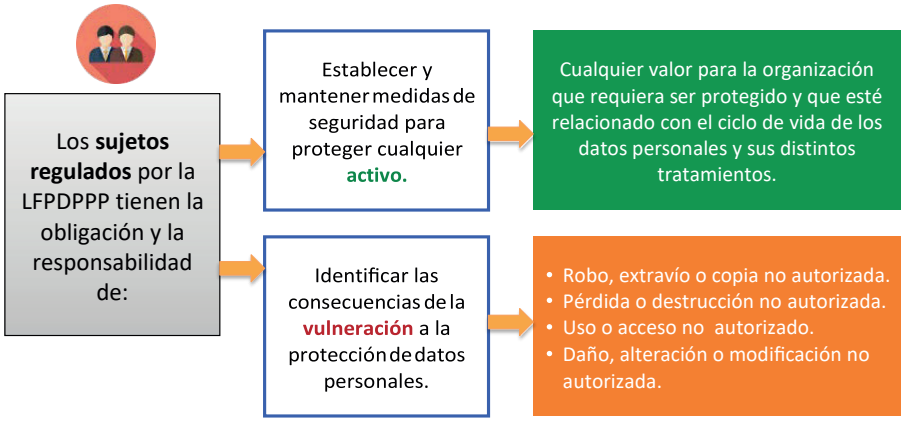
¿Ha recibido curso de capacitación con relación al tratamiento de datos personales? Si la respuesta es afirmativa, mencione cuál.

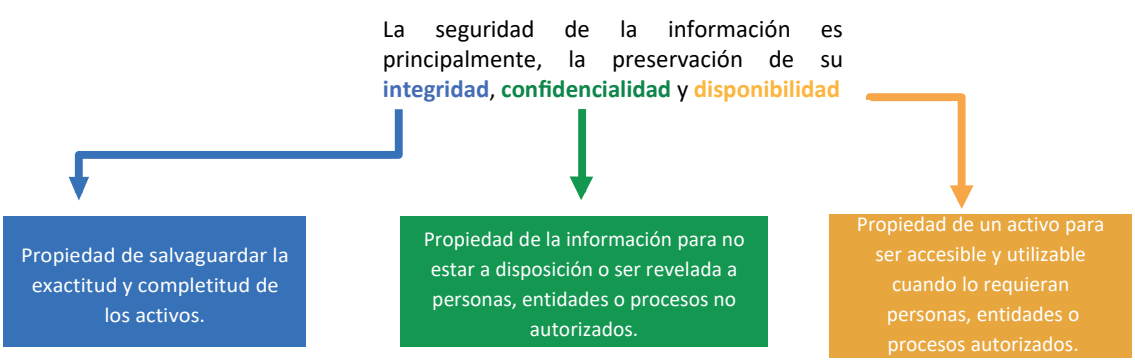
.....

.....

.....

Para concluir el módulo 2, se presenta un resumen con los contenidos que se revisaron.





Evaluación de avance

Instrucciones

Con la intención de verificar su nivel de conocimiento, marque con una “X” si la oración es verdadera o falsa.

Núm.	Afirmación	V	F
1	El Reglamento de la LFPDPPP, en su Artículo 61 establece acciones para la seguridad de los datos personales, entre otras, elaborar un inventario de datos y de sus medios de almacenamiento.		
2	Una amenaza se refiere a una circunstancia o evento con la capacidad de causar daño a una organización y puede ser solamente de origen humano, accidental, y provenir de adentro de la organización.		
3	El Artículo 63 del Reglamento de la LFPDPPP, establece el robo, extravío o copia no autorizada como algunos de los tipos de vulneraciones a la seguridad de los datos personales.		
4	El medio de almacenamiento físico de los datos personales, es todo recurso inteligible a simple vista y con el que se puede interactuar exclusivamente mediante un aparato que procese su contenido para examinar, modificar o almacenar datos personales.		

Para validar sus respuestas, consulte en el siguiente vínculo electrónico:


3
Módulo

Módulo 3

Acciones para la seguridad de los datos personales en posesión de los particulares.

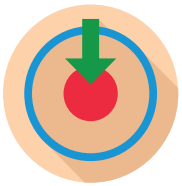
Objetivo particular:

Al finalizar el módulo, el lector diferenciará las fases del ciclo **PHVA** (Planificar, Hacer, Verificar, Actuar), que le permita adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), en cumplimiento de la legislación; a fin de proveer un marco de trabajo para el tratamiento de datos personales, que contribuya a mejorar su protección, disminuir los riesgos en su entorno de trabajo y actuar con apego a la Ley.

Para iniciar con el módulo 3, revisaremos algunas definiciones que le serán de utilidad para la secuencia de actividades a realizar.

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

Si quiere conocer más de las recomendaciones en materia de Seguridad de Datos Personales, visite: bit.ly/RecomendacionesSeguridadINAI2013



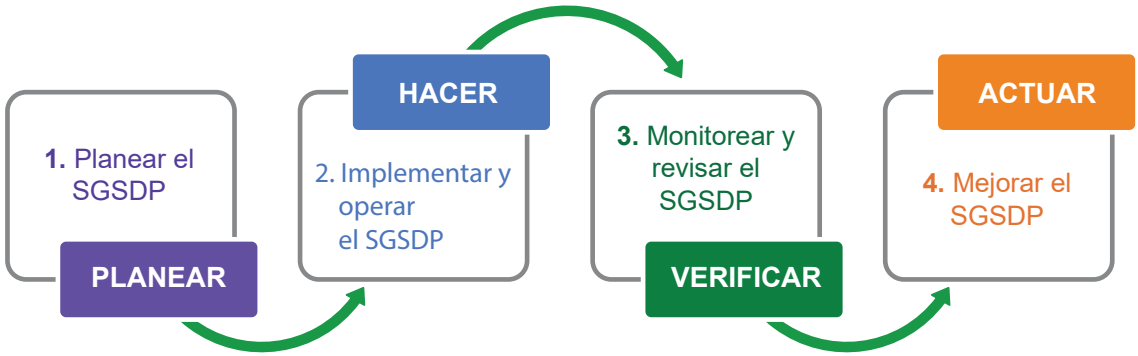
La gestión es un conjunto de actividades coordinadas para dirigir y controlar un proceso o tarea. Un sistema es un conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo. Por lo tanto, un **Sistema de Gestión (SG)** se define como un conjunto de elementos y actividades interrelacionadas para establecer metas y los medios de acción para alcanzarlas.

Un sistema de gestión apoya a las organizaciones en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr con éxito sus actividades, ya que está diseñado para mejorar continuamente el desempeño de una empresa u organización, mediante la consideración de las necesidades de todas las partes interesadas.

En particular, el **SGSDP** tiene como objetivo proveer un marco de trabajo para el tratamiento de datos personales que permita mantener vigente y mejorar la protección de datos personales para el cumplimiento de la legislación y fomentar las buenas prácticas, por lo que es indispensable conocer cada uno de los momentos que requiere la instrumentación de ese sistema, para su buen funcionamiento.

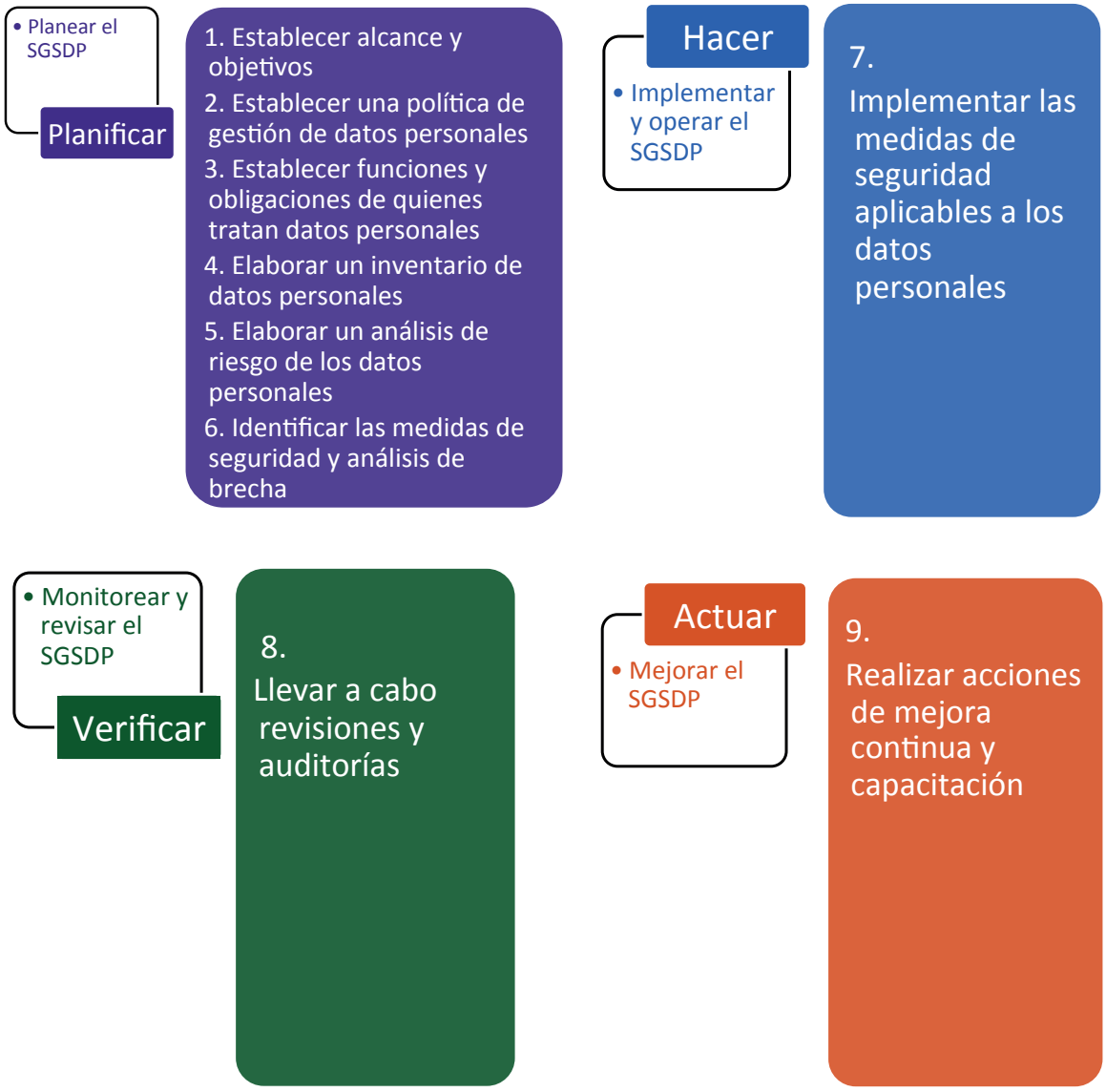
El Sistema **(PHVA)** cuenta con cuatro fases para su desarrollo:

Las cuatro fases del SGSDP



Cada una de estas fases sigue la lógica de la planeación estratégica. Entendemos por estrategia al conjunto de acciones que se llevan a cabo para lograr un objetivo. La palabra **estrategia** proviene del griego y significa literalmente “guía de los ejércitos”: ΣΤΡΑΤΗΓΙΚΗΣ: Stratos (ejército) + Agein (conductor, guía).

Cada una de estas fases, a su vez supone la realización de algunos pasos, que a continuación se describen:



Es importante establecer un plan para la instrumentación de un sistema, pero antes, recuerde que los datos personales que se encuentran bajo su posesión, están protegidos por las leyes, y que en todo momento debe tener presente los activos con que cuenta su empresa u organización, las amenazas, la vulnerabilidad y el impacto para la generación de escenarios de riesgo.

Retomando el video que se presentó en el módulo 1, en el que un empleado dió información confidencial y la envió por medios electrónicos sin salvaguardar su plena seguridad, se destaca que siempre hay que tomar en cuenta el impacto, es decir, una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

El impacto es la medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

Para reflexionar sobre las medidas de seguridad y el impacto que podría tener no cumplir con ellas, tome como ejemplo el problema del Licenciado Gómez, quien no sabía lo que había pasado con el expediente del Señor Martínez, debido a que:

El mes pasado, el Licenciado Gómez llegó tarde a su trabajo pues una cuestión con la salud de su hijo le había impedido presentarse a tiempo para la reunión de seguimiento. Aquel día la Licenciada Cabrera, Jefa de Unidad, le había solicitado a uno de los pasantes entregarle todos los expedientes del Licenciado Gómez, argumentando que los requería para la reunión. Una vez pasada la reunión, Juan el pasante, se lo devolvió a Guadalupe, la secretaria.

En virtud de que el expediente no estaba, el Licenciado Gómez decidió regresar con su cliente para proponerle una reunión posterior y darle continuidad a su trámite, con ello buscaba ganar tiempo para encontrar la información del Señor Martínez, posteriormente regresó a su oficina muy enfadado y angustiado. Buscó en su computadora los datos de registro de la propiedad de su cliente a fin de encontrar la forma de recuperar los documentos extraviados, la información que encontró fue que la propiedad ya estaba a nombre de otra persona.

Después de buscar el expediente y preocupado porque no aparecía por ningún lado, decidió exponer la situación a la Licenciada Cabrera, su jefa. Tocó a su puerta y le pidió unos minutos para platicar con ella sobre el asunto, trató de explicar la situación y le comentó que el expediente no estaba, entonces, la Licenciada Cabrera lo escuchaba con atención y parecía muy intrigada por lo sucedido, cuando el Licenciado Gómez le dijo que la propiedad estaba a nombre de otra persona, ella se enfadó, le dijo que eso no podía pasar y debía encontrar el expediente para resolver pronto el problema antes de que llegara a oídos del Notario. El Licenciado Gómez, más preocupado que antes, regresó a su oficina y siguió buscando.

Luego de un buen rato, entre unos papeles viejos encontró el expediente completo, casualmente, estaba fuera de lugar, y él no podía explicar qué era lo que había ocurrido, buscó a Marco, su amigo en el Registro Público de la Propiedad y de Comercio y le pidió ayuda para rastrear la propiedad e iniciar el trámite correspondiente, quien ingresó a la base de datos, y en efecto, la propiedad estaba a nombre de un tal Señor Manuel Sánchez, ¿pero cómo pudo pasar eso? aparecía una operación de compraventa hace apenas dos semanas. La propiedad se había vendido, el Licenciado

Gómez supo entonces que se había cometido un fraude y era obvio que su cliente no sabía nada al respecto.

Esto sí era un problema mayúsculo ¿qué debía hacer? ¿notificar a su jefa? ¿hablar con la Gerente Jurídica? ¿buscar directamente al Notario? Pensó que lo correcto era hablar con su jefa, pero el problema excedía las dimensiones de cualquier otra situación en la que había estado, así que decidió escalar el problema e ir a hablar con la Gerente, quien trataba los problemas de mayor monta en la Notaría, debía iniciar una averiguación, y encontrar todas las pruebas para eximirse de la responsabilidad.

Si su dispositivo cuenta con internet, puede reproducir el siguiente video[3], o bien consulte el vínculo electrónico:
https://youtu.be/hRsvqyS07fY

Ya que conoce un poco más del problema con el que estamos trabajando, es importante que identifique otro aspecto relevante para la evaluación del riesgo que pueden correr los datos personales, para lo cual, será importante conocer el flujo de los datos en su empresa u organización.

A continuación, conoceremos algunos elementos de la fase planeación.

Para planear es necesario que conozca cómo se tratan los datos personales en su entorno laboral, identificar la información con la que se cuenta y qué procesos al interior de éste implican el tratamiento de datos personales.

Repase la siguiente lista de los criterios a considerar:

[3] INAI [inaimexico]. (2017, Diciembre). Parte 2 medidas de seguridad dirigido a sujetos regulados [Archivo de video]. Recuperado de https://youtu.be/hRsvqyS07fY

1. De dónde se obtienen los datos personales (directamente del titular, a través de una transferencia o fuente de acceso público, entre otros);

2. Las unidades de negocio o departamentos que tratan datos personales para los servicios que ofrecen o actividades que realizan;

3. En particular, qué personas de la organización están autorizados a tratar los datos personales;

4. Las finalidades del tratamiento de los datos personales;

5. Con quién se comparten los datos personales (encargados o transferencias) y para qué se comparten;

6. En dónde y cómo se almacenan los datos personales;

7. Los procedimientos, mecanismos y tecnología utilizados para el tratamiento de datos personales;

8. Cuánto tiempo se conservan los datos personales, y

9. Los procedimientos para su destrucción.

Ejercicio de reflexión

Instrucciones.
Revise de nuevo la lista, pensando en el problema del Licenciado Gómez. Con base en la situación que ya conoce, ¿identifique qué deficiencias en el tratamiento de los datos personales hubo en la Notaría?

.....

.....

.....

.....

Con esta reflexión, revise el flujo con las acciones para la implementación de las medidas de seguridad, piense de qué manera se emplean o llevan a cabo estas medidas en su propio espacio de trabajo.

Una vez que ha identificado las etapas para la implementación de las medidas, a continuación se describen las preguntas a las que habrá de responder en cada una de ellas, mismas que se consideran en el **Manual en Materia de Seguridad de Datos Personales para MIPYMES y Organizaciones Pequeñas**.

Etapa 1: Identificación del flujo de los datos personales			
Pregunta 1: ¿Qué tipo de datos personales recabo?	Pregunta 2: ¿Cómo recabo los datos personales?	Pregunta 3: ¿Dónde se almacenan los datos personales?	Pregunta 4: ¿Quién tiene permiso para acceder o manejar los datos personales?

Etapa 2: Evaluación de las medidas de seguridad básicas		
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

Etapa 3: Plan de trabajo		
Selección de las acciones prioritarias	Periodo de cumplimiento de las acciones	Recursos humanos y materiales destinados a las acciones

Etapa 4: Mejora continua	
Implementación de todas las medidas de seguridad básicas	Modelo de madurez

Las acciones para implementar medidas de seguridad consideran cuatro etapas: identificar flujos de los datos personales, evaluar, elaborar plan de trabajo y mejora continua.

Seguramente ha podido identificar las medidas de seguridad faltantes para la protección de los datos personales que posee en su entorno de trabajo.

Responder a las preguntas de la tabla anterior:

¿Qué tipo de datos personales recabo?

.....

.....

.....

¿Cómo recabo los datos personales?

.....

.....

.....

¿Dónde se almacenan los datos personales?

.....

.....

.....

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

.....

.....

.....

Estas preguntas le ayudaran a identificar el flujo de los datos

Las acciones para implementar medidas de seguridad consideran cuatro etapas: identificar flujos de los datos personales, evaluar, elaborar plan de trabajo y mejora continua.

En la Notaría del problema de análisis de este curso, es evidente el fallo en la seguridad de los datos personales en su posesión derivado de un flujo de datos desordenado o descuidado. Además, conocer qué tipo de datos personales se tiene, para qué se emplean, cuánto tiempo se tienen, cómo se destruyen, son todos elementos muy importantes para analizar el riesgo que corren.

A su vez, y con base en la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales, misma que podrá consultar en todo momento en el repositorio del Campus Iniciativa Privada del CEVINAI. En ella podrá identificar escenarios de riesgo que es un paso importante para poder instrumentar un sistema de gestión para la seguridad de los datos personales.

Para mejorar el tratamiento de datos personales en su empresa u organización, realice el ejercicio de identificación de flujo de datos personales con la información que tiene de su entorno laboral.

Ejercicio de trabajo 5. El flujo de los datos.

Instrucciones.
Elabore la siguiente lista, utilizando como ejemplo su entorno laboral.
Trate de identificar con qué datos personales cuentan y el flujo que siguen éstos.

El flujo de los datos personales	
Elementos del flujo de datos	En mi entorno laboral
1. ¿De dónde se obtienen los datos personales (directamente del titular, a través de una transferencia o fuente de acceso público, entre otros)?	
2. Las unidades de negocio o departamentos que tratan datos personales para los servicios que ofrecen o actividades que realizan.	
3. En particular, qué personal de la organización está autorizado a tratar los datos personales.	
4. Las finalidades del tratamiento de datos personales.	
5. ¿Con quién se comparten los datos personales y para qué se comparten?	
6. ¿En dónde y cómo se almacenan los datos personales?	
7. Los procedimientos, mecanismos y tecnología utilizados para el tratamiento de datos personales.	
8. ¿Cuánto tiempo se conservan los datos personales?	
9. Los procedimientos para su destrucción.	

Una vez que conoce el flujo de los datos personales que se tratan en su empresa u organización, le será más fácil identificar los riesgos que podrían causar vulneraciones a la seguridad de los datos personales.

Para una revisión a fondo, consulte el Artículo 57 del Reglamento de la LFPDPPP.

Reglamento de la LFPDPPP.

Capítulo III
De las Medidas de Seguridad en el Tratamiento de Datos Personales

Artículo 57. El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales.

Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.

La información presentada a continuación, corresponde al análisis de riesgo de una empresa.

Una empresa ficticia que denominaremos AudiDatos, cuyo ejemplo se utilizará para fines didácticos, cuenta con medidas de seguridad tales como un sistema de control antiincendios y gafetes para identificar a todos los empleados, que son revisados por un guardia que trabaja de planta en el edificio. El personal de mantenimiento ha reportado humedad en las paredes del baño contiguo a la oficina donde se almacenan los archiveros con expedientes.

Desde que se compró el equipo de cómputo no se han hecho compras de ninguna licencia de software, el equipo de cómputo no está conectado a reguladores de voltaje y aunque los gerentes de vez en cuando copian la base de datos de clientes en dispositivos extraíbles, no cuentan con un procedimiento de respaldos periódicos del contenido del equipo.

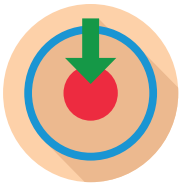
Todo el personal trabaja con entusiasmo y diligencia, sin embargo, hay rumores de que uno de los Técnicos en Audiometría está molesto con su Gerente. El siguiente ejemplo muestra la forma en la que deben analizarse los riesgos de los datos personales:

Activo	Amenazas	Vulnerabilidad	Impacto
Expediente de personal	Tuberías antiguas	Humedad	Daño
Resultado de estudios	Falta de suministro eléctrico	Equipo susceptible de variación de voltaje	Alteración o modificación
Base de datos de prospectos de clientes	Empleado descontento con su Gerente	Falta de vigilancia en la entrada	Robo
Computadora	Corrupción de datos	Falta de respaldos	Pérdida

Además, todo plan debe:

a. Estar orientado a la acción.
b. Integrar la prevision.
c. Ser un proceso constructivo y dinámico.
d. Reducir riesgos.

Cuando hablamos de **riesgo de seguridad**, nos referimos al potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización. Para saber más de este tema, revise la siguiente información.



Hay algunas medidas que se pueden instrumentar para identificar y reducir los riesgos; una vez realizada la identificación de los escenarios de vulneración o riesgo, que se entiende como todo proceso para encontrar, enlistar y describir los elementos del riesgo, es necesario **valorarlo**.

Aceptar el riesgo supone entonces una decisión informada para coexistir con un nivel de riesgo, una vez hecho lo anterior se debe tratar el riesgo, es decir, instrumentar procesos para modificar el nivel de riesgo, algunos de estos procesos son:

Riesgo es el potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

Compartir: Es un proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

Evitar: Se refiere a llevar a cabo acciones para retirarse de una situación de riesgo o decisión para no involucrarse en ella, o por lo menos, reducirla.

Reducir: Implica tomar acciones para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

Retener: Es aceptar la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.

Finalmente, el **riesgo residual** es el remanente después de tratar el riesgo, cualquier riesgo, además, se debe comunicar, que no es más que compartir o intercambiar información entre la alta dirección, custodios y demás involucrados acerca del riesgo.

En este sentido, pueden tomarse o llevarse a cabo acciones de previsión que vayan reduciendo los riesgos en el tratamiento de los datos personales y disminuir la posibilidad de que ocurra una vulneración a su seguridad. Por ejemplo, en el problema que estamos revisando, es claro que nadie llevó a cabo un análisis de riesgo, y las consecuencias de eso para una empresa u organización, o para el titular de los datos, pueden ser catastróficas.

Usando como base esta información y el ejemplo de la empresa ficticia AudiDatos que acaba de revisar, realice la siguiente actividad. Puede regresar a los módulos anteriores si necesita repasar algunos de los conceptos que se muestran en esta tabla.

Ejercicio de trabajo 6. Análisis de riesgo.

Instrucciones.
Complete la tabla utilizando el problema del Licenciado Gómez. Piense en la situación idónea, es decir, la forma en la que él y todos en su espacio de trabajo pudieron prever la situación en la que ahora se encuentran.

Tabla 1			
Activo	Amenazas	Vulnerabilidad	Impacto

Instrucciones.
Ahora, siguiendo el ejemplo anterior, le pedimos por favor, conteste la siguiente tabla, donde puede describir de que forma puede prevenir el tratamiento inadecuado de los datos personales que posee en su entorno de trabajo.

Tabla 2			
Activo	Amenazas	Vulnerabilidad	Impacto

Con el ejercicio anterior pudo clasificar el tipo de activos que posee su empresa u organización, lo que estaría cumpliendo con la identificación del tipo de datos personales, y con ello, determinar cuál es el flujo que siguen, como sabe, ello le permitirá afinar también y tener más claridad para anticipar qué riesgos corren.

Recuerde que al revisar la información, siempre debe considerar el cumplimiento de la LFPDPPP, su Reglamento y otras normas relacionadas que obligan a proteger los datos personales en posesión de los particulares.

En los ejercicios anteriores pudo identificar riesgos, amenazas y flujo de datos, ahora conocerá la primera fase de instrumentación Sistema de Gestión de Seguridad de Datos Personales para lo cual, deberá identificar el tipo de datos personales que actualmente posee y conocer si éstos son o no sensibles.

De acuerdo con la lectura del **Artículo 3** de la **LFPDPPP**, se entiende por datos personales sensibles aquellos que afecten a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Ahora identifique si los datos personales que posee su empresa u organización son o no sensibles. Como un ejercicio adicional puede visitar la aplicación desarrollada por el INAI, a fin de hacer una evaluación de los datos que posee su empresa u organización en:

La aplicación, tiene como propósito promover la importancia de la protección de los datos personales, a través de una estimación económica del riesgo vinculado al tipo de datos tratados y a la percepción del titular con relación al responsable del tratamiento de sus datos personales, tomando en cuenta que muchas veces son la moneda de cambio de bienes y servicios que se ofrecen como gratuitos.

Otro aspecto relevante en la protección de los datos personales es saber cómo se recaban, por ejemplo, conocer en qué tipo de formatos se almacenan. En este sentido, elaborar un listado de todos los documentos, plantillas, formularios, físicos o electrónicos en los que se registran los datos personales identificados puede ser de gran utilidad.

Implementar medidas de seguridad por capas, estableciendo filtros, es una recomendación que podría tomar en cuenta.

Un ejemplo de lo anterior, es establecer un primer filtro para acceder a los datos personales que es un sitio de resguardo, como una oficina con sistema de alarma; el siguiente filtro es el acceso al medio de almacenamiento, mediante un archivero bajo llave con los expedientes de los pacientes; y finalmente el acceso al formato, es decir, los documentos que componen el expediente de un paciente en específico.

La implementación de medidas de seguridad debe reflejar los recursos disponibles, humanos, económicos, de conocimiento y de tiempo con los que cuenta la organización; conociendo lo anterior, podrá diseñar un adecuado plan de trabajo, que deberá contener al menos:

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

Las empresas 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.

Los controles pueden consultarse en el **Manual en Materia de Seguridad de Datos Personales para MIPYMES y Organizaciones Pequeñas**, disponible en el repositorio del Campus Iniciativa Privada del CEVINAI, y que podrán serle de utilidad toda vez que están enfocados en la menor inversión monetaria a cambio de que se fomente la cultura de la protección de datos personales.

También deberá instrumentar medidas correctivas en caso de vulneraciones de seguridad, como se sugiere en el **Artículo 66 del Reglamento de la LFPDPPP**.

Artículo 66 del Reglamento de la LFPDPPP.

En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.

Nunca olvide que la seguridad de los datos personales no es un proyecto que se instrumenta y sucede por única vez, sino un esfuerzo constante, es decir, como en el ciclo **PHVA**, deberá regresar una y otra vez las fases que lo integran.

En la fase de planeación también es relevante conocer las medidas de seguridad que existen y las que faltan, a esto se le llama **análisis de brecha**.

Podemos decir que 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.

Puede instrumentar algunas de las herramientas que hemos revisado, a fin de hacer el análisis de brecha en su propio entorno de trabajo, para lograrlo le proponemos la siguiente actividad:

¡La seguridad de los datos personales es un esfuerzo permante!

Ejercicio de trabajo 7. Análisis de brecha.

Instrucciones.
Conteste la siguiente tabla, de acuerdo a las medidas que identifique en su espacio de trabajo.

Análisis de Brecha (Medidas de seguridad existentes vs medidas de seguridad faltantes)				
Código	**Pregunta o Control**	**¿Existente?**		
		Si	**No**	**Observaciones**
A	**Medidas de seguridad basadas en la cultura del personal**			
A.1	¿Pone atención en no dejar a la vista datos personales y lleva registro de su manejo?			
A.1.1	¿Cuenta con una política de escritorio limpio?			
A.1.2	¿Tiene hábitos de cierre y resguardo de documentos?			
A.1.3	¿Sus impresoras, escáneres, copiadoras y buzones, permanecen limpios de documentos?			
A.1.4	¿Realiza alguna gestión de bitácoras, usuarios y acceso?			
A.2	¿Tiene mecanismos para eliminar de manera segura la información?			
A.2.1	¿Realiza la destrucción segura de documentos?			
A.2.2	¿Realiza una eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico?			
A.2.3	¿Establece periodos de retención y destrucción de información?			
A.2.4	¿Toma precauciones con los procedimientos de reutilización?			
A.3	¿Ha establecido y documentado los compromisos respecto a la protección de datos personales?			
A.3.1	¿Informa al personal sobre sus deberes mínimos de seguridad y protección de datos personales?			
A.3.2	¿Fomenta la cultura de la seguridad de los datos personales?			
A.3.3	¿Se difunden noticias en temas de seguridad?			
A.3.4	¿Realiza acciones de capacitación para prevenir al personal sobre la Ingeniería Social?			
A.3.5	¿Se cuenta con medidas para asegurar la protección de datos personales en subcontrataciones?			
A.4	¿Existen procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?			
A.4.1	¿Cuenta con un procedimiento de notificación de vulneraciones?			
A.4.2	¿Realiza revisiones y auditoria?			
A.5	¿Realiza respaldos periódicos de los datos personales?			

B	Medidas de seguridad en el entorno de trabajo físico			
B.1	¿Tiene medidas de seguridad para acceder al entorno de trabajo físico?			
B.1.1	¿Cuenta con alertas en el entorno de trabajo?			
B.1.2	¿Mantiene registros del personal con acceso al entorno de trabajo?			
B.2	¿Tiene medidas de seguridad para evitar el robo?			
B.2.1	¿Cuentan con cerraduras y candados?			
B.2.2	¿Existen elementos que permitan disuadir un posible robo?			
B.2.3	¿Se realizan acciones para minimizar el riesgo oportunista?			
B.3	¿Cuida el movimiento de información en entornos de trabajo físicos?			
B.3.1	¿Cuenta con sistemas de aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico?			
B.3.2	¿Mantiene en movimiento sólo copias de la Información y no el elemento original?			
B.3.3	¿Usa mensajería certificada?			
C	**Medidas de seguridad en el entorno de trabajo digital**			
C.1	¿Realiza actualizaciones al equipo de cómputo?			
C.2	¿Revisa periódicamente el software instalado en el equipo de cómputo?			
C.3	¿Tiene medidas de seguridad para acceder al entorno de trabajo electrónico?			
C.3.1	¿Actualmente cuenta con uso de contraseñas y/o cifrado?			
C.3.2	¿Sus contraseñas son sólidas?			
C.3.3	¿Realiza bloqueo y cierre de sesiones?			
C.3.4	¿Cuenta con un sistema de administración de usuarios y accesos?			
C.4	¿Revisa la configuración de seguridad del equipo de cómputo?			
C.5	¿Tiene medidas de seguridad para navegar en entornos digitales?			
C.5.1	¿Cuenta con herramientas antimalware y de filtrado de tráfico?			
C.5.2	¿Dispone de reglas de navegación segura?			
C.5.3	¿Establece reglas para la divulgación de información?			
C.5.4	¿Hace uso de conexiones seguras?			
C.6	¿Cuida el movimiento de información en entornos de trabajo digitales?			
C.6.1	¿Valida el destinatario de una comunicación?			
C.6.2	¿Cuenta con elementos de seguridad de la información enviada y recibida?			

La parte final de este módulo, tiene como propósito el desarrollo de algunos ejercicios que le serán de utilidad para la creación de su propio Sistema de Gestión de Seguridad de Datos Personales (SGSDP).

Para mayor referencia de estos aspectos, puede revisar a fondo la **Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales** que se encuentra disponible en el sitio: http://cevinafaiprivada.ifai.org.mx. Por ahora, la realización de las siguientes actividades será suficiente para que tenga una idea general de lo que deberá hacer para instrumentar ese sistema en sus diferentes fases.

Antes de mostrar los ejercicios y a manera de recapitulación de las cuatro fases que ha estado revisando, recuerde lo siguiente:

La primera fase de **planeación** supone estructurar un plan para identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por la organización. En la segunda fase, **hacer**, se refiere a implementar y operar el **Sistema de Gestión de Seguridad de Datos Personales (SGSDP).**

Es el momento en que se deberán poner en marcha las medidas de seguridad que hayan resultado aplicables según el análisis de riesgo realizado en la fase de planeación.

En la tercera fase, **verificar**, se monitorea y revisa el **Sistema de Gestión de Seguridad de Datos Personales (SGSDP),** es decir, es cuando se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.

En la cuarta fase, **actuar**, se mejora el **Sistema de Gestión de Seguridad de Datos Personales (SGSDP)** y se lleva a cabo la capacitación, es cuando se adoptan las medidas correctivas y preventivas en función de los resultados de la revisión o verificación efectuadas, o de otra información relevante, para lograr la mejora continua. Una parte fundamental de esta fase es la capacitación del personal.

Al terminar las fases, vuelve a inicar el ciclo, de ahí lo que se decía antes, que es un esfuerzo continuo y no algo que sucede por única vez. Dicho lo anterior, a fin de que pueda llevar a cabo una tarea específica en lo que respecta a la creación del sistema de gestión en su propia empresa u organización, realice la actividad final.

Ejercicio de trabajo 8.- Consideraciones para un sistema de gestión.

Instrucciones.
Para establecer los objetivos y procesos necesarios que lleven a su empresa u organización a obtener los resultados esperados, respecto a la protección y seguridad de los datos personales, a partir del contexto general de la información y los procesos de su espacio de trabajo, escriba lo que se le solicita. Puede apoyarse en la “Guía para Implementar un Sistema de Seguridad de Datos Personales”.

Ejercicio de trabajo correspondiente a la Fase 1: Planear el SGSDP

A. Alcance y objetivos

Instrucciones

En esta primera fase para la creación del SGSDP, es necesario que delimite el ámbito de aplicación que involucra el tratamiento de los datos personales en su empresa u organización. Para ello, complete la siguiente información:

Nombre de las áreas y personas que, como parte de sus actividades laborales, tratan datos personales	Personas con quienes se comparten los datos y propósito del tratamiento	Lugar y tiempo de almacenamiento de los datos personales	Procedimiento para el tratamiento y destrucción de los datos personales

Ahora determine el objetivo del **SGSDP** con base en los factores contractuales, legales, tecnológicos y regulatorios del modelo de negocio; los cuales se detallan en la **"Guía para Implementar un Sistema de Seguridad de Datos Personales"**

Objetivo del SGSDP

.....

.....

.....

.....

.....

.....

B. Política de gestión de datos personales

Instrucciones

Elabore la propuesta de una política de gestión de datos personales que establezca el compromiso de cumplir con la legislación vigente sobre la protección de datos personales por parte de todos los involucrados en el tratamiento.

Para poder elaborar esta propuesta, primero debe definir los alcances y objetivos de la gestión de los datos personales, posteriormente, el responsable deberá emitir e implementar dicha política, darle seguimiento, mantener su implementación a través del tiempo y actualizar o realizar ajustes cuando sea necesario.

La política debe tener muy bien definidos su alcance y objetivo, y recordar que aplica a todos los datos personales que son tratados en la organización dentro de los distintos procesos y finalidades convenidas con los titulares.

La política debe establecer el compromiso de cumplir con la legislación en protección de datos personales por parte de todos los involucrados en el tratamiento, por lo que debe ser comunicada a los mismos, e incluir al menos las siguientes reglas:

a. El cumplimiento de todos los principios que establece el artículo 6 de la Ley.
b. Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable (principio de licitud).
c. Sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley (principio de consentimiento).
d. Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (principio de información).
e. Procurar que los datos personales tratados sean correctos y actualizados (principio de calidad).
f. Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron (principio de calidad).
g. Tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos organizacionales (principio de calidad).
h. Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad (principio de finalidad).
i. No obtener los datos personales a través de medios fraudulentos (principio de lealtad).
j. Respetar la expectativa razonable de privacidad del titular (principio de lealtad).
k. Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad (principio de proporcionalidad).
l. Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación (principio de responsabilidad).
m. Establecer y mantener medidas de seguridad (deber de seguridad).
n. Guardar la confidencialidad de los datos personales (deber de confidencialidad).
o. Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos de la organización se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.
p. Mantener un inventario actualizado de los datos personales o de sus categorías que maneja la organización.
q. Respetar los derechos de los titulares en relación con su datos personales.
r. Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales.
s. Desarrollar e implementar un SGSDP de acuerdo a la política de gestión de datos personales, y
t. Definir las partes interesadas y miembros de la organización con responsabilidades específicas y a cargo de la rendición de cuentas para el SGSDP.

A continuación, elabore la propuesta de una política de gestión de datos personales atendiendo a las características y necesidades de su entorno de trabajo.

Propuesta de Política de Gestión de Datos Personales

.....

.....

.....

.....

.....

.....

C. Funciones y obligaciones de quienes tratan datos personales

Instrucciones

Enliste las principales funciones que deberá atender el responsable de tratar los datos personales. Recuerde que éstas deben asegurar que la gestión de los datos personales sea parte de los valores de la organización.

Funciones del Responsable de Tratar los Datos Personales

F1 .....

F2 .....

F3 .....

F4 .....

F5 .....

Ahora, defina las obligaciones del responsable de tratar los datos personales.

Obligaciones del Responsable de Tratar los Datos Personales

1. .....

.....

.....

2. .....

.....

.....

3. .....

.....

.....

4. .....

.....

.....

5. .....

.....

.....

D. Inventario de datos

Instrucciones

Con base en la “Guía para Implementar un Sistema de Seguridad de Datos Personales”, en el siguiente formato elabore un inventario de los sistemas de tratamiento de datos personales que utilice su empresa u organización. Considere que se debe mantener actualizado y estar vinculado con la información básica que permita conocer el tipo de tratamiento al que son sometidos los datos personales y que se relaciona directamente con su ciclo de vida: obtención, almacenamiento, uso, divulgación, bloqueo, cancelación, supresión o destrucción.

Inventario de los sistemas de tratamiento de datos personales	
Obtención	
Almacenamiento	
Tipo de uso	
Divulgación	
Bloqueo	
Cancelación / Supresión / Destrucción	

E. Análisis de riesgo de los datos personales

Instrucciones

Con el propósito de que los responsables determinen las características del riesgo que puede tener mayor impacto sobre los datos personales que tratan, y con la finalidad de que prioricen y tomen la mejor decisión respecto a los controles más relevantes e inmediatos a implementar, realice el siguiente ejercicio en el que deberá identificar en su organización, los criterios de impacto y los criterios de aceptación del riesgo.

A reserva de su lectura a la **"Guía para Implementar un Sistema de Seguridad de Datos Personales"**, a manera de resumen podemos señalar que hay dos tipos de criterios de evaluación del riesgo: los de impacto y los de aceptación.

Criterios de impacto: Se definen en términos del posible nivel de daño y perjuicio al titular causado por un evento negativo a la seguridad de los datos personales, considerando:

- El valor de los datos para la organización.
- El incumplimiento con las obligaciones legales y contractuales relacionadas con el titular.
- Vulneraciones de seguridad (art. 63 del Reglamento).
- Daño a la integridad de los titulares de datos personales.
- Daño a la reputación de la organización.

Criterios de aceptación del riesgo: La organización podría aceptar o no ciertos niveles de riesgo, siempre y cuando la naturaleza del riesgo, sus consecuencias o su probabilidad sean consideradas como muy poco significativas.

Estos criterios dependen de las políticas y objetivos de la organización, así como, de las partes interesadas, considerando que:

- Se debe expresar el beneficio o el riesgo estimado para la organización, aplicando diferentes criterios de aceptación correspondientes al riesgo. Por ejemplo, riesgos que pueden resultar del incumplimiento a la Ley que no pueden ser aceptados.

- Se deben incluir múltiples umbrales, correspondientes a diferentes niveles de aceptación, previendo que los responsables acepten riesgos sobre esos niveles en circunstancias específicas.

- Los criterios de aceptación del riesgo pueden incluir requerimientos para una gestión futura, por ejemplo, un riesgo puede ser aceptado si hay aprobación y el compromiso de la alta Dirección para tomar acciones que permitan reducirlo a un nivel aceptable dentro de un periodo establecido posteriormente.

Para definir todo criterio de aceptación del riesgo es importante considerar:

- Política(s) de la organización respecto al tratamiento de datos personales.
- Aspectos legales y regulatorios.
- Operaciones.
- Tecnología.
- Finanzas.
- Factores sociales y humanitarios.

Estos criterios corresponden a todo el posible daño a los titulares.

Valoración Respecto al Riesgo

Cuando se tienen definidos criterios de evaluación del riesgo, por ejemplo ¿cuál sería el riesgo estimado para la organización de no poner el aviso de privacidad a disposición de sus clientes? o ¿qué personas se verían afectadas y de qué forma si se sustrajera la base de datos con la nómina de la organización?

Se tiene que valorar el riesgo de forma cuantitativa, cualitativa o ambas, para atenderlo en la fase de implementación.

La valoración del riesgo identifica los activos existentes, las amenazas aplicables, y los escenarios de vulneración. Asimismo, determina las consecuencias potenciales y prioriza los riesgos derivados respecto al contexto de la organización y los criterios de evaluación del riesgo.

Esta valoración del riesgo debe considerar:

- El establecimiento y mantenimiento de criterios de aceptación de riesgos.
- La determinación de los criterios para evaluar los riesgos.
- Asegurar que las diferentes evaluaciones del riesgo generen resultados consistentes válidos y comparables.

Estos criterios deberían estar formalmente documentados y ser utilizados como directriz para valorar el riesgo.

Una vez que conoce los conceptos anteriores, le pedimos establezca los criterios de evaluación del riesgo de la seguridad de los datos personales de su empresa u organización. Escríbalos en el siguiente formato.

Criterios de Impacto	Criterios de Aceptación del Riesgo

a. Después de definir los criterios de evaluación de riesgo de la seguridad de los datos personales, identifique los activos existentes, las amenazas aplicables y los escenarios de vulneración. Determine las consecuencias potenciales y vierta su información en el siguiente formato.

Identificación de activos y amenazas			
Activos existentes	Amenazas aplicables	Escenarios de vulneración	Consecuencias potenciales

F. Identificación de medidas de seguridad y análisis de brecha

Instrucciones

Como último paso, deberá implementar las medidas de seguridad administrativas, técnicas o físicas que considere permitirán la disminución de los riesgos.

En la "**Guía para Implementar un Sistema de Seguridad de Datos Personales**" encontrará el anexo D, en el cual se explica cada uno de los dominios.

Una vez que ha leído el Anexo D, en el siguiente cuadro se muestran los diez dominios principales, marque con una X si lo está aplicando o no en su entorno de trabajo y describa qué objetivo de control es el que ha implementado.

Medidas de Seguridad			
Dominios principales	Sí	No	
Políticas del SGSDP	Sí	No	
Cumplimiento legal	Sí	No	
Estructura organizacional de la seguridad	Sí	No	
Clasificación y acceso de los activos	Sí	No	
Seguridad del personal	Sí	No	
Seguridad física y ambiental	Sí	No	
Gestión de comunicaciones y operaciones	Sí	No	
Control de acceso	Sí	No	
Desarrollo y mantenimiento de sistemas	Sí	No	
Vulneraciones de seguridad	Sí	No	

Ejercicio de trabajo correspondiente a la Fase 2. Implementar y operar el SGSDP

A. Implementación de las medidas de seguridad aplicables al tratamiento de los datos personales.

Instrucciones

En la segunda fase del SGSDP deberá implementar las medidas de seguridad que hayan resultado aplicables según el análisis de riesgo realizado en la fase de planeación. De las cuatro opciones, en el siguiente formato, seleccione las que considere pertinentes (reducir, retener, evitar o compartir), describa el riesgo que identifica en su organización y defina los motivos de su viabilidad.

Opciones de Tratamiento de Riesgo	Describa el Riesgo	Motivo de Viabilidad
Reducir el riesgo		
Retener el riesgo		
Evitar el riesgo		
Compartir el riesgo		

Fase 3. Monitorear y revisar el SGSDP

A. Evaluación y medición de los resultados de las políticas, planes, procesos y procedimientos.

Instrucciones

En la tercera fase del SGSDP deberá revisar su funcionamiento respecto a la política establecida. En el siguiente cuadro indique como llevaría a cabo el monitoreo y explique por qué.

Revisión de los factores de riesgo	Auditoría	Vulneraciones a la seguridad de los datos personales	Motivo del monitoreo

Fase 4. Mejorar el SGSDP

A. Mejora continua y capacitación.

Instrucciones

Con el propósito de mantener actualizado el **SGSDP**, indique las acciones que propone para incluir la protección de los datos en la cultura de su empresa u organización. Recuerde atender las recomendaciones que se presentan en la "**Guía para Implementar un Sistema de Seguridad de Datos Personales**".

	Acción 1	Acción 2	Acción 3	Acción 4	Acción 5
Mejora continua con medidas preventivas y correctivas					
Capacitación del personal para mantener la vigencia del SGSDP					

Una vez que ha realizado este ejercicio y conoce los momentos clave a para la creación de un SGSDP, a continuación, le presentamos el resumen de los temas que se revisaron en este módulo:

Para cada tipo de **activo** es fundamental **identificar** la **vulnerabilidad** de que puede ser objeto, a fin de contrarrestar posibles **amenazas** a los datos personales y así, minimizar **riesgos**.

* La seguridad de los datos personales es un **esfuerzo permanente**

Análisis de brecha

=

Conocer las medidas de seguridad existentes y las que faltan

También es indispensable establecer un **sistema de seguridad de datos personales**, pues el impacto de perder, alterar o hacer uso indebido de la información, puede reflejarse en el daño, en mayor o menor medida, a los activos y al nivel de objetivos alcanzados por una organización.

Planificar	•**Identificar** políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por la organización (meta)
Hacer	•**Implementar y operar** las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior
Verificar	•**Evaluar y medir** los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, para verificar que se haya logrado la mejora esperada
Actuar	•**Adoptar medidas** correctivas y preventivas, en función de los resultados y de la revisión, o de otra información relevante, para lograr la mejora continua.

Evaluación de avance

Instrucciones

Con la finalidad de verificar el nivel de conocimiento que desarrolló durante el módulo, lea las afirmaciones de la columna izquierda y relaciónelas con la información de la columna derecha.

Núm.	Afirmaciones	Respuesta		
1	Son las fases para instrumentar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP).		a.	Verificar.
2	En un SGSDP, es el paso en el que se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, a fin de confirmar que se haya logrado la mejora esperada.		b.	Identificación de los escenarios de vulneración o riesgo.
3	Alude a todo proceso para encontrar, enlistar y describir los elementos del riesgo.		c.	Sistema de Gestión de la Seguridad de los Datos Personales (SGSDP).
4	Conjunto de elementos y actividades interrelacionadas cuyo objetivo es proveer un marco de trabajo para el tratamiento de datos personales.		d.	Planificar, hacer, verificar y actuar.

Para validar sus respuestas, consulte en el siguiente vínculo electrónico:

Conclusiones

Hasta ahora hemos trabajado en dos ejercicios, el primero fue el problema del Licenciado Gómez y el segundo la aplicación de conceptos y herramientas en su propio espacio de trabajo.

El primero, como problema eje, fue el elemento articulador de los contenidos y temas a revisar. Después se analizaron los riesgos en el tratamiento de los datos personales que tenía la Notaría y qué pudo hacerse para prevenir esos riesgos, por último, el ejercicio que se realizó en el módulo anterior, siguiendo como ejemplo el problema de la Notaria, donde los jefes deberían llevar a cabo acciones para eficientar las medidas de seguridad.

Durante el análisis del problema del Licenciado Gómez, se conoció la situación, pero al mismo tiempo, usted realizó analogías con su propio entorno laboral y con la información que tenía y la que faltaba por conocer, formuló hipótesis sobre el origen del problema, las posibles causas y diversas ideas para resolverlo.

En un tercer momento recurrió a aquellos conocimientos de los que disponía, a los detalles del problema que conocía y que podría haber utilizado para su posterior resolución. Cuando determinó aquello que no sabía del problema y lo que necesitaría para resolverlo, también pudo formular preguntas orientadas a la solución de la situación.

Correspondía entonces una siguiente fase, plantear soluciones; como se mencionó anteriormente, la solución de un problema parte de un plan inicial e indispensable. Asimismo, supone realizar una investigación para poder definir adecuada y concretamente el problema a resolver y en el que se va a centrar esa investigación. Después, toda solución de un problema implica un período de trabajo; obtener la información necesaria, estudiarla y comprenderla, pedir ayuda si es necesario, posteriormente presentar la solución al problema y mostrar resultados. Finalmente, el proceso vuelve a comenzar con la formulación de otro problema.

Siguiendo esta estructura, que podrá utilizar siempre que se enfrente a una situación problemática, terminaremos entonces como empezamos:

El Licenciado Gómez, si recuerda en donde nos quedamos, presentó a la Gerente Jurídica el caso del Señor Martínez. Obviamente llegó a oídos del Notario y de las autoridades, se llevó a cabo una revisión pormenorizada del asunto, se revisaron los videos de las cámaras de seguridad, de las que nadie en la Notaría tenía conocimiento y se descubrió que la Licenciada Cabrera había cometido un delito.

El día de la reunión, a la que el Licenciado Gómez no asistió, tomó el expediente del Señor Martínez y llevó a cabo la venta indebida de la propiedad, evidentemente se inició un proceso penal en su contra.

En lo relativo a la protección de datos personales, es importante señalar que el Artículo 63 de la LFPDPPP, establece las conductas que constituyen infracciones, así como las sanciones que pudieran corresponder al caso concreto. Por lo tanto, previa denuncia ante el INAI y en caso de resultar procedente, podría derivar en la imposición de una sanción, además de la pérdida de la credibilidad que pudiera impactar en la Notaría lo que se traduciría a su vez en un menoscabo patrimonial.

Si su dispositivo cuenta con internet, puede reproducir el siguiente video[4], o bien consulte el vínculo electrónico: https://youtu.be/mSV-7VEjSBE

Como ellos, usted tendrá también mucho por hacer a fin de poner en marcha lo que ha aprendido en este curso.

¡Le deseamos éxito en esta labor!

[4] INAI [inaimexico]. (2017, Diciembre). Parte 3 medidas de seguridad dirigido a sujetos regulados [Archivo de video]. Recuperado de https://youtu.be/mSV-7VEjSBE

Manual de consulta del curso
en materia de “Medidas de seguridad”
Se terminó de imprimir en los talleres de
Impresora y Encuadernadora Progreso, S.A. de C.V.
(IEPSA),
San Lorenzo 244, C.P. 09830, Ciudad de México,
en diciembre de 2017.

El tiraje fue de 5,000 ejemplares.

Edición a cargo del
Instituto Nacional de Transparencia, Acceso a la
Información y Protección de Datos Personales (INAI)