Instituto Nacional Electoral

Manual en materia de Seguridad de Datos Personales

Documento integrante de la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad de la Protección de los Datos Personales, perteneciente al Programa para la Protección de los Datos Personales 2018-2023, aprobado en sesión extraordinaria del Comité de Transparencia del 8 de noviembre de 2018.

V 5.1

Figura 1. Modelo de Protección de Datos Personales del Instituto Nacional Electoral

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FIRMA DEL RESPONSABLE
1.0	Creación del documento con base en el Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas [1] del INAI.	Jazmín Torres Blanco	Febrero 2018	
2.0	Modificación del documento.	Jazmín Torres Blanco	Febrero 2019	
2.0	Adaptación al Programa de Protección de Datos Personales del Instituto.	Karen Guillermina López García	Febrero 2019	
2.0	Revisión del documento.	Blanca Estela Carrillo Sánchez	Febrero 2019	
2.1	Se incorpora en la introducción la aclaración que los casos prácticos y sus soportes documentales son ilustrativos. Mención de la herramienta para análisis de brecha en la página 47.	José Antonio Galván Estrada	Octubre 2019	
2.2	Actualización del documento.	Fabiola Paulina Vázquez Ramírez	Enero 2020	
2.2	Actualización del documento.	Diana Gabriela Noemí Benítez Mejía	Enero 2020	
2.2	Revisión de forma, fondo del documento y normatividad.	Fabiola Paulina Vázquez Ramírez	Febrero 2020	
3.0	Revisión de forma y fondo. Se complementa manual con los	Diana Gabriela Noemí Benítez Mejía	Febrero 2020	

[1] Disponible en: http://inicio.ifai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FIRMA DEL RESPONSABLE
	temas de seguridad, cómputo en la nube. Se agregan temas de estándares y análisis de riesgos.			
3.0	Revisión y actualización de documento.	Blanca Estela Carrillo Sánchez	Marzo 2020	
3.0	Revisión de forma y fondo. Actualización de términos electrónico a digital, formato a soporte.	Diana Gabriela Noemí Benítez Mejía	Marzo 2020	
4.0	Revisión de fondo, forma y actualización de documento	Diana Gabriela Noemí Benítez Mejía	Abril 2020	
5.0	Revisión y actualización de documento.	Blanca Estela Carrillo Sánchez	Agosto 2020	
5.1	Revisión y actualizaciones de forma.	Jazmín Torres Blanco	Marzo 2023	

CONTENIDO

INTRODUCCIÓN

El 8 de noviembre de 2018, mediante Acuerdo INE-CT-ACG-PDP-004-2018 el Comité de Transparencia aprobó el **Programa para la Protección de Datos Personales del Instituto Nacional Electoral**, el cual incluye la Estrategia para el cumplimiento de los Deberes de Seguridad y Confidencialidad, cuya finalidad es determinar las acciones concretas a seguir por parte de la Unidad Técnica de Transparencia y Protección de Datos Personales (UTyPDP) y de las áreas responsables, respecto al tratamiento de los datos personales en lo referente al Título Segundo, Capítulo II de la Ley de Datos.

Con relación a lo antes expuesto, la UTyPDP consideró necesaria la elaboración del presente manual, con la finalidad de que el personal de este Instituto se familiarice y sensibilice con la seguridad de la información y la protección de los datos personales para implementar medidas de seguridad efectivas que contribuyan a mitigar las posibles vulneraciones a la seguridad de los datos personales en posesión de este organismo público autónomo.

Lo anterior sin olvidar que son causas de sanción el no establecer las medidas de seguridad como lo señala la Ley en sus artículos 31, 32 y 33.

El presente manual cuenta con los siguientes apartados:

- Las principales obligaciones para la protección de los datos personales,
- Los riesgos a los que se exponen en el caso de omisión,
- Una guía para mejorar la protección de los datos mediante cuatro etapas:
    - La identificación del flujo de los datos personales;
    - La identificación de las medidas de seguridad básicas;
    - La elaboración de un plan de trabajo y
    - Acciones para la mejora continua.

Todos los casos prácticos desarrollados en el presente manual son de carácter ilustrativo, para poder acceder a las herramientas y documentos completos, deberá consultar el **Procedimiento para elaborar el Documento de Seguridad,** el cual puede solicitar a la Unidad de Transparencia.

OBJETIVO

Orientar al personal, que por sus funciones traten datos personales, en el cumplimiento de los Deberes de seguridad y confidencialidad, de acuerdo con la normatividad vigente en la materia.

ALCANCE

Dirigido al personal de los órganos ejecutivos, técnicos y de vigilancia, en materia de transparencia, y de control, que por sus funciones traten datos personales en el INE.

REFERENCIAS NORMATIVAS

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (La ley).
- Lineamientos Generales de Protección de Datos Personales en el Sector Público (Los lineamientos).
- Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales (Reglamento).

TÉRMINOS Y DEFINICIONES

Además de las definiciones previstas en el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y de las señaladas en el Programa para la Protección de Datos Personales del Instituto Nacional Electoral, para efectos del presente Manual se entenderá por:

Amenaza: cualquier situación, acción o acontecimiento no deseado e inesperado con la capacidad de ocasionar un daño o consecuencias adversas para un bien o una persona y está asociada con la explotación de una vulnerabilidad. La amenaza es que una entidad (alguien, o algo) identifique una vulnerabilidad y la use contra la organización.

Ciclo de vida de la información: Las etapas de la información desde su captación hasta su borrado o conservación.

Empleado: Personal de la rama administrativa, personal de la rama administrativa de los OPLE, personal del servicio nacional electoral, los prestadores de servicios por honorarios, los prestadores de servicio social, entre otros.

Incidente: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de una organización, que afecte la confidencialidad, la integridad o la disponibilidad de la información. Es un riesgo materializado.

Sistema informático: Es el conjunto de partes interrelacionadas, hardware, software y de recurso humano que permite almacenar y procesar información.[2]

Riesgo: Probabilidad de que una entidad (algo o alguien), conocida como agente de amenaza, explote una vulnerabilidad.

Vulnerabilidad: es la falta, defecto o falla de una medida de seguridad o una debilidad de un bien o persona. Las vulnerabilidades afectan a los bienes de una organización (activos), pero también pueden darse sobre un procedimiento destinado a protegerlo.

Vulneración: Es un incidente de seguridad que afecta a los datos personales en cualquier fase de su tratamiento.

[2] Definición obtenida de https://www.ecured.cu/Sistema_inform%C3%A1tico

1 CONCEPTOS GENERALES

La ley platicada

El deber de seguridad

La Ley, en su artículo 31, señala que todos los sujetos obligados que usen datos personales deben de establecer y mantener, medidas de seguridad técnicas, administrativas y físicas para proteger los datos personales que estén en su posesión, garantizando su confidencialidad, integridad y disponibilidad.

En los Lineamientos, en el Capítulo II, se detallan las actividades con base en las cuales se deben adoptar las medidas de seguridad. Es decir, si sabemos dónde y cómo recabamos, almacenamos, utilizamos y eliminamos la información, entonces sabremos dónde necesitamos establecer medidas de seguridad y cuáles son las mínimas con las que debemos contar.

Este manual te ayudará a entender cómo se tratan los datos personales y qué hacer para cumplir con los deberes de seguridad y confidencialidad, cuando:

- Usan datos personales de: menores de edad, ciudadanos, empleados, prestadores de servicio social, entre otros, para diversas finalidades.
- Tienen pocas nociones sobre el tema de protección de datos personales y seguridad de la información.

1.1 IMPORTANCIA DE LOS DATOS PERSONALES Y SU PROTECCIÓN

Las instituciones deben conocer y mostrar interés en la protección de los datos personales, por las siguientes razones:

- La protección de datos personales es un derecho humano de los titulares que se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales y en la normatividad aplicable y, a su vez, es una obligación para quienes los tratan.
- Para ayudar a prevenir y mitigar los riesgos una vulneración a la seguridad de los datos personales.
- Para aumentar la competitividad, mejorar los procesos de las áreas del Instituto y el nivel de confianza de los titulares de los datos personales.

Dentro de los beneficios que se obtienen al establecer y mantener medidas de seguridad, así como la documentación respectiva, se encuentran, tanto el aumento de la certidumbre como la confianza de los titulares de los datos personales.

Por otro lado, se mejoran los procesos de Instituto y la eficacia del tratamiento de los datos personales en su posesión.

La ley platicada

El principio de responsabilidad

La Ley, en su artículo 16, establece los principios para la protección de los datos personales, entre los cuales se encuentra la responsabilidad. El Reglamento en su artículo 30, señala que el Instituto dará cumplimiento al principio de responsabilidad, acreditando el apego a los principios, deberes y obligaciones establecidos en la normatividad y aplicando los mecanismos establecidos en la Ley.

Algunos de los mecanismos que se deben de cumplir, de acuerdo con el artículo 30 de la Ley son: la elaboración de políticas y programas de protección de datos personales, el establecimiento de sistemas de supervisión y vigilancia como auditorías para comprobar el cumplimiento y la realización de programas de capacitación y actualización del personal sobre las obligaciones y deberes.

Asimismo, los Lineamientos en el artículo 46, señalan que en la elaboración de mecanismos y políticas se debe de considerar, entre otras cosas, el desarrollo tecnológico y las técnicas existentes; la naturaleza, el contexto, los alcances y finalidades del tratamiento de los datos.

1.2 PRINCIPALES OBLIGACIONES PARA LA PROTECCIÓN DE DATOS PERSONALES

La ley establece como uno de sus objetivos el tratamiento legítimo de datos personales, lo que implica que deban ser utilizados sólo para las finalidades que el titular ha consentido al entregar su información.

Importante

El aviso de privacidad

El aviso de privacidad es el documento a través del cual, los responsables informan a los titulares cómo y para qué usarán sus datos personales. Su elaboración y puesta a disposición es una de las obligaciones principales de todo aquél que trate datos personales y cumple con el principio de información establecido en la Ley.

El aviso de privacidad deberá mostrarse al momento previo de recabar los datos personales y puede encontrarse en forma física, digital o en cualquier soporte documental que permita su eficaz comunicación.

Esta obligación tiene vigencia desde el 27 de enero de 2017.

Para más información y herramientas para la elaboración del aviso de privacidad, puedes visitar el sitio web del INAI o consultar lo señalado en los artículos 27 y 28 de la Ley y los artículos 26 al 45 de los Lineamientos.

El mantenimiento de forma segura de las bases de datos que contienen datos personales y sus sistemas de tratamiento -a través de los cuales se obtienen, almacenan, procesan y/o comparten datos personales- puede ser una tarea compleja, que requiere tiempo, recursos y conocimientos especializados.

Esta tarea se facilita cuando quien trata datos personales identifica adecuadamente el uso de la información en cada uno de los procesos del Instituto.

Importante

Base de datos y Sistema de datos personales

Una **base de datos** es el conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterio determinados, con independencia de forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

A partir de una o varias bases de datos, es posible generar un subconjunto de datos –que serán empleados para finalidades diferentes de la base de datos origen-, a las cuales les llamaremos sub-bases de datos. Cada base de datos, incluidas las sub-bases, deben contar con un **dueño o propietario, quien elaborará los avisos de privacidad y el documento de seguridad**.

Un **sistema de datos personales** es un sistema automatizado o manual, a través del cual se realiza el tratamiento de los datos personales almacenados en su base de datos. También **poseen un dueño o propietario** -que puede o no coincidir con los propietarios de la base que trata-, **y son quienes elaboran las cedulas de identificación de cada sistema de datos personales**.

1.3 MODELO DE CICLO DE VIDA DE LA INFORMACIÓN

De conformidad con lo señalado en el artículo 59 de los Lineamientos, el responsable deberá considerar el ciclo de vida de los datos personales recabados u obtenidos, así como identificar los riesgos inherentes a los mismos y los involucrados en su tratamiento, considerando al menos los siguientes elementos: su obtención, almacenamiento, uso, acceso, manejo, aprovechamiento, monitoreo y procesamiento, bloqueo, cancelación, supresión o destrucción de los datos personales.

En este sentido, el ciclo de vida de la información se refiere a los estados por los que pasa la información desde su creación/obtención hasta su destrucción/conservación, en los cuales, en cada una de sus fases, se deben observar los principios señalados en la Ley de Datos.

El Modelo de Ciclo de Vida de la Información del Instituto[3], consta de cinco fases, las cuales se describen a continuación:

- **Fase 1. Creación/colecta/captura:** Esta fase se considera como la inicial del ciclo de vida y se asocia con el acto de crear, adquirir o incorporar información nueva que no existía con anterioridad en el área.

  En esta fase, los principios que deben ser observados son los de licitud, finalidad, lealtad, calidad, consentimiento, proporcionalidad, información y responsabilidad.

- **Fase 2. Procesamiento**
  a) **Mantenimiento de datos/pre-procesamiento:** Es el proceso de envío de la información recién capturada al almacenamiento persistente (discos duros, discos ópticos, memorias USB, archivos físicos, entre otros) que incluye procesos para acondicionar y normalizar la información antes de su incorporación a la base de datos.

     El principio que debe ser observado en esta etapa es el de calidad.

  b) **Almacenamiento:** Es el acto de hacer persistente la información para su uso regular.

     Los principios que deben ser observados son finalidad y calidad.

[3] Para ahondar en el modelo puede consultar el documento denominado "Modelo de Ciclo de Vida de la Información".

c) **Síntesis de datos/transformación:** Corresponde con la creación de nueva información o extracción del valor a partir de la información pre-existente capturada con anterioridad.

Los principios que deben ser observados son los de finalidad e información.

d) **Uso de la información:** En esta fase la información recabada (haya o no sido transformada y/o sintetizada), se aplica en la ejecución de las tareas del área.

Los principios que deben ser observados son los de calidad, información y finalidad.

- **Fase 3. Transferencia/publicación/revelación:** Esta fase corresponde cuando la información es enviada fuera del área.

  En esta fase, los principios que deben ser observados son los de finalidad e información.

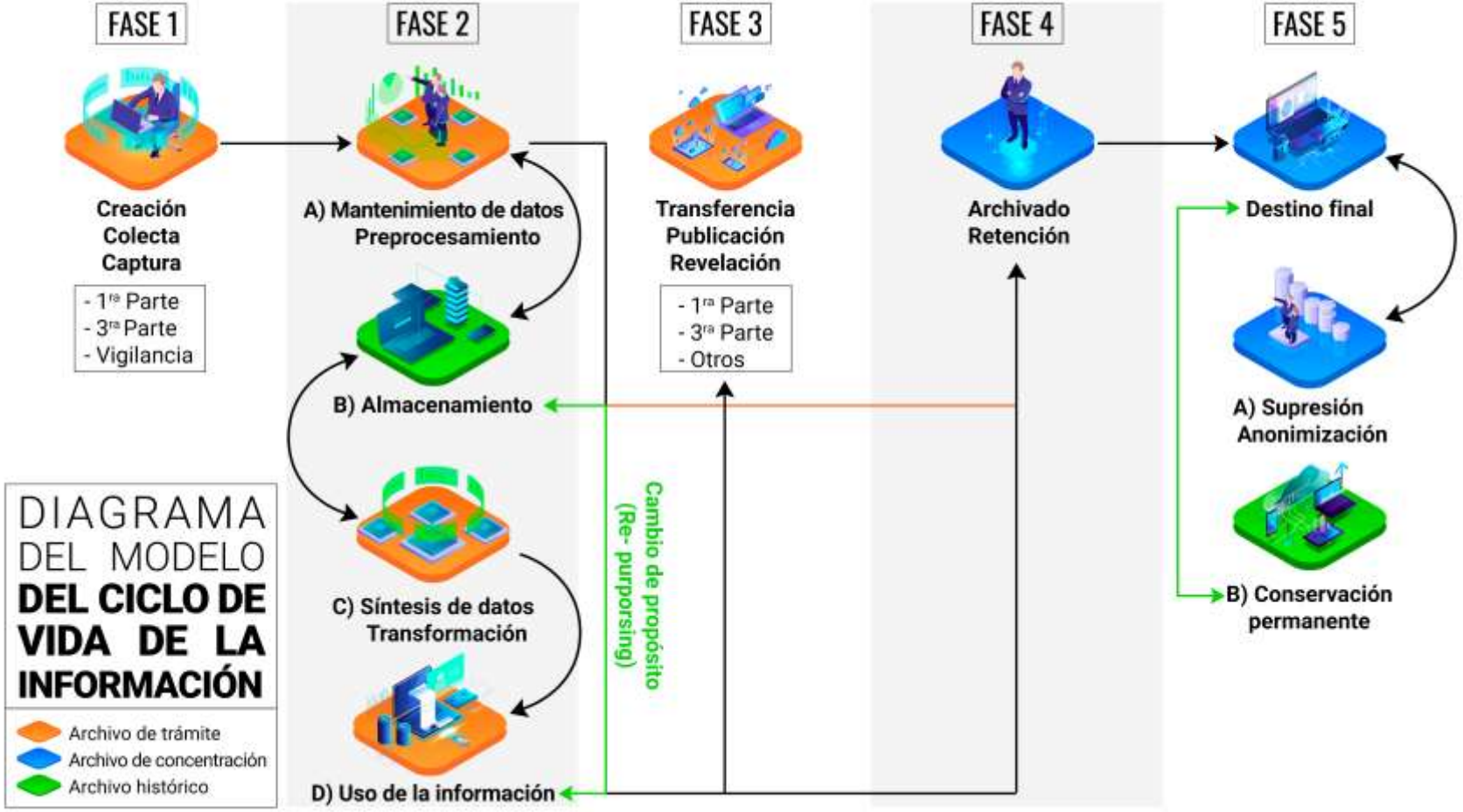
- **Fase 4. Archivado/retención:** En esta fase se lleva a cabo el traslado de toda la información digital de los ambientes de producción o los documentos de archivo -*que haya cumplido con lo señalado en el Catálogo de Disposición Documental*- a un entorno de almacenamiento secundario para poder ser accedidos en caso de que sea necesario.

  En esta fase, los principios que se deben observar son los de finalidad, consentimiento e información.

- **Fase 5. Destino final:** Con base en el Catálogo de Disposición Documental, se debe identificar si la información -*que contiene el dato personal*- se suprime o se conserva como indefinida.
  a) Supresión/anonimización (disociación)
  b) Conservación permanente

  En esta etapa, los principios que deben ser observados son los de finalidad, consentimiento, información y responsabilidad.

El diagrama del modelo se muestra a continuación:



1.4 LOS RIESGOS A LOS QUE ESTÁN EXPUESTOS LOS DATOS PERSONALES

Duda razonable

¿De quién o de qué protejo los datos personales?

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

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

El objetivo de implementar medidas de seguridad es que cada una de ellas ayude a reducir el riesgo al que están expuestos los datos personales durante su ciclo de vida, ya que esto podría provocar un daño a otros derechos de las personas.

Las medidas de seguridad también ayudan a que, en caso de presentarse un incidente, se reduzca el daño a los titulares y al Instituto.

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

Espionaje, es decir, actividades que tienen un objetivo especìfico como daño a una organización, obtener ventaja comercial o ganancias.

Por ejemplo, personas externas a la organización o delincuentes que tratan de obtener bases de datos de forma ilegal, entre otros.

Situación fortuita, en la que la vulneración puede darse sin que haya sido planteada.

Por ejemplo, un empleado que no bloquea su computadora, corre el riesgo de que le copien archivos con datos personales en una memoria USB o que simplemente alteren la información con la que estaba trabajando.

Descuido o desastres naturales, por ejemplo:

1. Alteración o eliminación de un expediente por error humano, o por falla en los equipos de cómputo.
2. Pérdida de información como consecuencia de un terremoto o inundación.

La ley platicada: Tipos de vulneraciones

El artículo 38 de la Ley de Datos, establece que se deben considerar, al menos, las siguientes vulneraciones de seguridad que pueden ocurrir en cualquier momento del tratamiento de los datos personales:

Caso Práctico

El riesgo de los datos personales de los aspirantes y prestadores de servicio social en custodia de la Institución "X"

La Institución "X" celebró convenios con universidades públicas para implementar un programa de servicio social, por lo que diversos estudiantes han entregado sus documentos (mismos que contienen datos personales) con la finalidad de ingresar. Sin embargo, al realizar el proceso de selección de aspirantes y al dar seguimiento a los trámites de los prestadores de servicio social, la Institución detectó posibles vulneraciones.

Para disminuir la probabilidad de que ocurran vulneraciones, la Institución se ha dado a la tarea de identificar posibles incidentes:

Tipo de Vulneración	Incidente
La pérdida o destrucción no autorizada de los expedientes	Que una persona malintencionada *destruya los archivos físicos o digitales* que contienen los expedientes de los aspirantes o prestadores de servicio social, lo cual podría impedir al estudiante ingresar al programa, obstaculizaría su servicio social, o en su caso retrasaría los trámites para obtener su carta de liberación.
El robo, extravió o copia no autorizada	Que personal del departamento encargado que trata los datos personales extravié el equipo en el cual se almacenan los datos de los aspirantes y prestadores de servicio social y que caiga en manos de alguien que pueda hacer una copia no autorizada de la base de datos y utilizarla para finalidades diferentes para las que fueron recabados. O en su caso, extraviar los documentos impresos que entregaron los estudiantes.
El uso, acceso o tratamiento no autorizado	Que un empleado de la Institución que trata los datos personales no bloquee su equipo al salir y como consecuencia un empleado no autorizado acceda a la base de datos de los aspirantes o prestadores de servicio social.
El daño, alteración o modificación no autorizada	Que una persona malintencionada modifique los datos del aspirante, como, por ejemplo: promedio, edad, créditos, experiencia; por lo que no podría ingresar al programa o sería canalizado a un área que no se apegue a su perfil.

Para ello, la Institución "X" llevará a cabo la implementación de mecanismos de seguridad que atiendan las vulnerabilidades que podrían originar estas vulneraciones.

Aprendizaje de la Institución "X"

La Institución "X", interesada en realizar un tratamiento responsable de los datos personales y tomando en cuenta las vulneraciones que otras Instituciones han sufrido, ha identificado algunas vulnerabilidades que podrían causar una vulneración a los datos personales que custodia. Al contemplar diversos escenarios, le será más fácil implementar medidas de seguridad.

El **Anexo D** contiene otros ejemplos de vulneraciones.

2 LA PROTECCIÓN DE LOS DATOS PERSONALES

La ley platicada: Acciones para la seguridad

La Ley, en su artículo 32, establece las siguientes actividades a considerar para la seguridad de los datos personales:

1. El riesgo inherente a los datos personales tratados y su sensibilidad,
2. El desarrollo tecnológico,
3. Las posibles consecuencias de una vulneración para los titulares,
4. Las transferencias de datos personales que se realicen,
5. El número de titulares,
6. las vulneraciones previas ocurridas en los sistemas de tratamiento, y
7. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión

A través de este manual, los responsables y encargados de los datos personales en las áreas del Instituto identificarán elementos de apoyo a cubrir en cada una de estas acciones y así generar un esquema de seguridad continuo, consistente y efectivo.

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

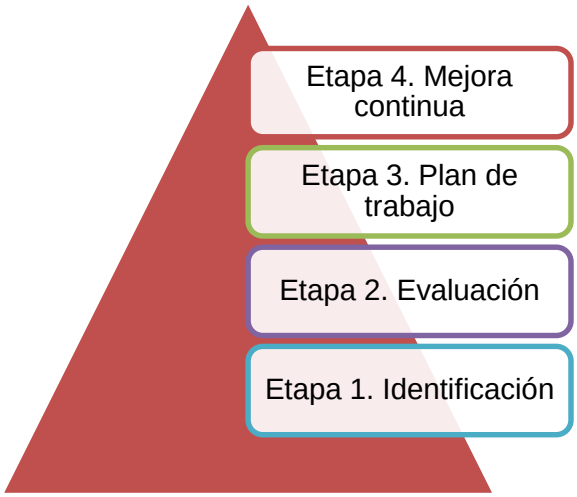
Las cuatro etapas en las que se divide este apartado son:

- Etapa 1. Identificación del flujo de datos personales.
- Etapa 2. Evaluación de las medidas de seguridad.
- Etapa 3. Plan de trabajo.
- Etapa 4. Mejora continua.

El objetivo de dividir en etapas es distribuir y facilitar la protección de los datos personales con las actividades relacionadas para alcanzar cada una de ellas y que lleven a los responsables y encargados a la madurez en la seguridad.

La pirámide que se muestra a continuación; ordena las cuatro etapas que los responsables y encargados deberán alcanzar para madurar en el tema de seguridad de los datos

personales, donde la etapa 1 es la base y en la cúspide se encuentra la etapa de la mejora continua.



Una vez que se avanzan las tres primeras etapas, en la mejora continua, se evalúa la eficacia y eficiencia de lo implementado en las etapas anteriores, y si requiere de alguna modificación.

Así como se observa en la pirámide, las etapas son acumulativas y no se puede avanzar a la siguiente sin cubrir adecuadamente la anterior.

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

Importante

El valor de documentar las acciones de seguridad

Uno de los principales obstáculos para la implementación de la seguridad en las Instituciones es la falta de documentación. La documentación debe demostrar el tratamiento legítimo de la información ante los titulares o las autoridades, así como tener mejores estrategias y soporte documental ante una vulneración a la seguridad de los datos personales.

Al tener la información exacta sobre sistemas, bases de datos y toda la infraestructura donde el área trata los datos personales y debidamente documentada, permite una pronta respuesta ante una vulneración, gestión de cambios, actualizaciones, entre otras acciones necesarias de mantenimiento o respuesta a incidentes.

2.1 Etapa 1. Identificación del flujo de los datos personales

Los responsables y encargados de las áreas del Instituto deberán contestar cada una de las preguntas de esta etapa para identificar con claridad el tratamiento de los datos personales, desde que los recaban hasta que los eliminan.

En esta sección, se detallan tres preguntas básicas para la identificación de flujo de los datos personales, las cuales son:

- Pregunta 1. ¿Qué tipos de datos personales recabo?
- Pregunta 2. ¿Cómo recabo los datos personales?
- Pregunta 3. ¿Quién tiene permiso para acceder a los datos personales?

Para auxiliar en la identificación del flujo de los datos personales, es de utilidad tener el diagrama a bloques del proceso del área responsable para poder identificar el flujo de los datos, así como las bases de datos involucradas.

2.1.1 Pregunta 1. ¿Qué tipos de datos personales recabo?

Tomando en consideración los principios de legalidad, proporcionalidad y finalidad, el objetivo es identificar qué tipo de datos personales se recaban en los distintos soportes que se utilizan, y lo más importante, si es necesario recabarlos o no, conforme a la finalidad establecida.

La respuesta a esta pregunta es un listado de todos los tipos de datos personales recabados y si son necesarios para que el Instituto pueda ofrecer productos y/o brindar servicios.

La ley platicada

Criterio de minimización

El artículo 25 de los Lineamientos establece que el responsable deberá realizar los esfuerzos razonables para limitar los datos personales al **mínimo necesario,** con relación a las finalidades que motivan su tratamiento.

Lo anterior, tiene relación con lo establecido en el artículo 25 de la Ley y en el artículo 24 de los Lineamientos, los cuales tratan el principio de proporcionalidad.

En este sentido, los responsables deben obtener los datos personales que son adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Se entenderá que se cumple lo anterior, cuando los datos son apropiados, indispensables y no excesivos conforme a las finalidades que motivaron su obtención, las cuales deben atender a las atribuciones con las que cuenta el responsable.

Caso práctico

Datos personales que recaba el programa de servicio Social de la Institución "X".

Mediante el aviso de privacidad, el programa de servicio social de la "Institución X" informa a los aspirantes y/o prestadores de servicio social cuáles son los datos que recaba y las finalidades relacionadas con su uso: ya sea para la generación de un expediente personal, reportes, evaluaciones, carta de inicio y carta de terminación, entre otras.

A continuación, en la tabla que se muestra, realiza el listado de todos los tipos de datos que recaba a través de soportes documentales y al terminar, realiza una evaluación para saber si utiliza y recaba esos datos de acuerdo con las finalidades previstas en su aviso de privacidad.

Datos personales recabados/obtenidos	¿Es necesario?	¿Por qué?
Datos de identificación		
Nombre	*En esta sección se indica si el dato recabado es necesario para los fines relacionados con su uso.* Sí	*El responsable deberá **justificar el motivo por el cual recaba u obtiene cada uno de los datos personales y por qué es necesario, así como señalar el fundamento legal** en el que se otorga la atribución para su tratamiento.* *Se debe mencionar la Ley, el artículo, inciso, fracción y párrafo correspondiente o bien el lineamiento, reglamento o procedimiento aplicable. En caso de no existir alguno de los anteriores, indicar el manual u otro documento aprobado por el titular que sustente el tratamiento. De esta manera, todos los datos personales que se recaben estarán respaldados por un fundamento legal.* El domicilio se recaba para registrar al prestador en el seguro de accidentes. Los datos X, Y, A, se recaban para identificación y registro del prestador en el sistema "Prestadores de servicio social" conforme a los artículos 2 y 3 p.II de los "Lineamientos de servicio social".
Domicilio	Sí	
Teléfono de casa y/o celular	Sí	
Edad	Sí	
Sexo	Sí	
Universidad	Sí	
Créditos	No	
Estado Civil	Sí	
Promedio	No	
Datos personales sensibles		
Información médica y/o del estado de salud física y/o mental	No	*De igual manera que en la sección de datos de identificación, se debe señalar el fundamento legal por el cual se recaban los datos y especificar aquellos utilizados.*
Opiniones y/o preferencias políticas	No	

Es importante señalar que los datos que se enlistan son un ejemplo, ya que se deben analizar todos los datos personales que son recabados u obtenidos para el caso en concreto, con su correspondiente justificación y normatividad.

En el análisis, la Institución "X" identifica que almacena en sus registros los créditos, el promedio, información médica y/o del estado de salud física y/o mental y las opiniones y/o preferencias políticas de los aspirantes a prestadores de servicio social, los cuales no son relevantes para el programa de servicio social, por lo que decide tomar las siguientes acciones al respecto:

- Dejar de solicitar a los aspirantes a prestadores de servicio social los datos innecesarios.
- Eliminar de la base de datos actual, los registros referidos a estos datos.
- Avisar a los aspirantes a prestadores de servicio social sobre los cambios en el aviso de privacidad.

Las Institución "X" podría incluso, darse cuenta de que no requieren ciertos medios de almacenamiento y optar por eliminarlos.

Con estas acciones la Institución "X" podrá canalizar mejor y enfocar sus esfuerzos en la protección de datos personales, pues no tendrá que almacenar datos que no requiere para la finalidad del programa, y así disminuirá el nivel de riesgo al que expone a los titulares y cumplirá el principio de proporcionalidad de la ley.

También se deberá tener cuidado y atención en la forma en la que se obtienen los datos, por ejemplo, la Institución "X" puede solicitar al aspirante a prestador de servicio social en la información médica el tipo de sangre de la persona, sin necesidad de solicitar un estudio de sangre.

El **Anexo A.1** muestra un **ejemplo** de listado general de los tipos de datos personales.

Asimismo, las áreas deberán identificar la categoría de los datos personales que son recabados, con la finalidad de conocer el nivel que le corresponde a cada dato personal –**estándar, sensible o especial**-.

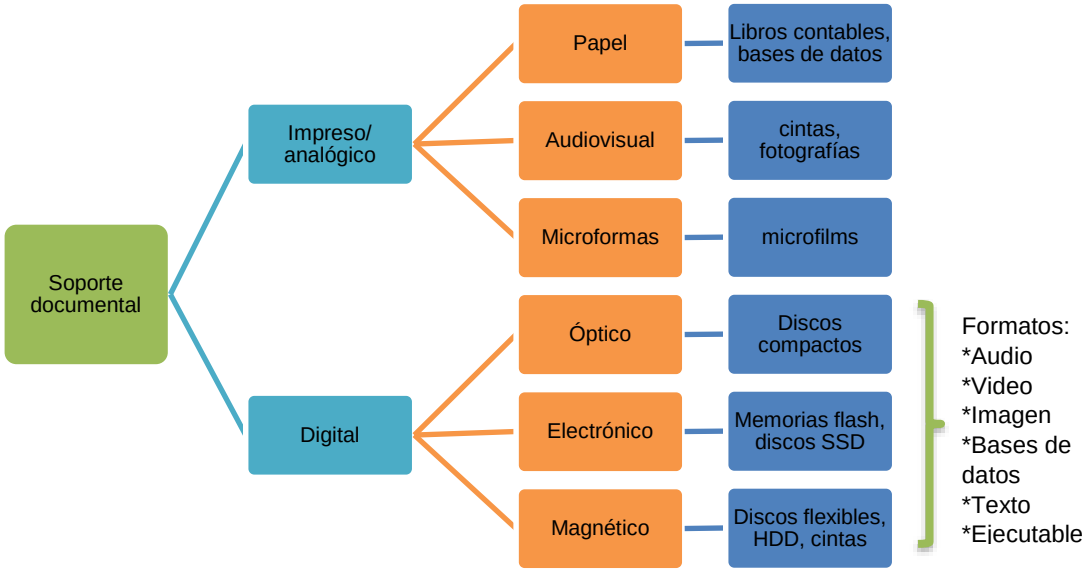
El **Anexo B.1**, contiene la categorización establecida por el INAI. Cabe señalar, que la categorización puede variar atendiendo al contexto de los datos personales.

Importante

Sitios, medios y soportes documentales

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

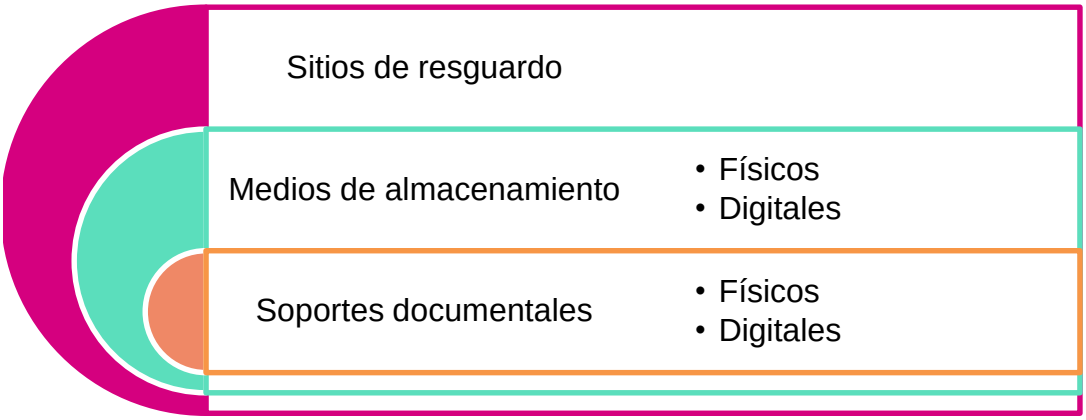
- **Sitio de resguardo:** Toda locación donde se resguarden los medios de almacenamiento, tanto físicos como digitales (por ejemplo, la oficina de la Institución o empresa o las instalaciones de un tercero).
- **Medio de almacenamiento físico:** Es todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales. Por ejemplo, los expedientes del personal almacenados en un archivero. En este sentido hay que considerar cuartos especiales, bóvedas, muebles, cajones y cualquier espacio donde se guarden soportes físicos, o bien equipo de cómputo u otros medios de almacenamiento de datos personales.
- **Medio de almacenamiento digital:** Es todo recurso al que se puede acceder mediante el uso de equipo 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*, discos duros extraíbles, entre otros. También podemos contemplar como medio de almacenamiento digital, el uso de servicios de almacenamiento en línea.
- **Soporte documental o material**: Es el medio en el cual está contenida la información y puede variar según los materiales y la tecnología empleada, por lo que puede ser impreso o digital, por ejemplo: papel, fotografías, filminas, cintas, plástico, metal entre otros que se muestran en la siguiente figura:



- **Formato**: Se refiere a las características que definen la forma en la que se codifica la información en soporte documental digital. Por ejemplo, los que se muestran en la figura anterior.

- **Soporte 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.
- **Soporte digital:** Define cómo se obtiene la información personal en formato digital, 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 los datos personales de lo particular a lo general, como se muestra a continuación:



En este ejemplo, a través de los soportes documentales físicos y digitales se obtienen los datos personales que se resguardan en medios de almacenamiento, que a su vez se encuentran ubicados en los sitios de resguardo. De esta manera se documentará el modelo, conforme se contestan las preguntas 2 y 3 que se encuentran en los puntos 2.1.2 y 2.1.3.

Una vez que se han identificado los sitios de resguardo, se debe precisar el medio de almacenamiento ya sea físico o digital, es decir, el contenedor o dispositivo en que son almacenados los datos y posteriormente la forma en que son guardados.

Este modelo nos permite implementar medidas de **seguridad por capas** de la siguiente manera:

- El primer filtro, es para acceder a los datos personales en un sitio de resguardo, por ejemplo, una oficina con sistema de alarma.
- El siguiente filtro, es el acceso al medio de almacenamiento, por ejemplo, un archivero bajo llave con los expedientes de los aspirantes o prestadores de servicio social,
- Finalmente, el acceso al soporte documental, por ejemplo, la base de datos o el formulario que contiene los datos personales de los aspirantes, protegidas con un usuario y contraseña para su acceso.

2.1.2 Pregunta 2. ¿Cómo recabo los datos personales?

El objetivo de esta pregunta es identificar en qué tipo de soportes documentales el responsable recaba y almacena los datos personales.

El responsable debe tener en una tabla todos los documentos, plantillas, formularios, físicos o digitales en los que se registran los datos personales identificados en la Pregunta 1.

Caso práctico

Cómo almacena la institución X los datos personales

La Institución "X" realiza un análisis del cómo están agrupados los datos personales y en qué **soporte documental y formato** se almacenan y utilizan en la Institución "X", detallando en la tabla que se muestra a continuación:

Soporte documental y formato	Físico	Digital
Correo		Mensajes, carpetas y documentos de aspirantes y prestadores de servicio social enviados y recibidos a la cuenta de correo electrónico designada para el programa.
Formularios	Soporte documental impreso que se entrega a los aspirantes para llenar.	
Hoja de calculo		serviciosocial.xls
Expedientes	Impresiones de los expedientes	Documentos de tipo: nombre_aspirante.doc o nombre_prestador.doc
Audios y/o video		Videos de vigilancia de la cámara en las instalaciones de la Institución.

Con el análisis, la Institución "X" identificó a simple vista, que en los soportes documentales digitales es donde se concentra la mayor parte de la información personal y también que los correos, hojas de cálculo y expedientes, son los soportes documentales en los que tratan mayor volumen de datos.

En el **Anexo A.2**, se proporciona una tabla en blanco similar a la de este caso práctico, para la elaboración de sus propias listas de soportes documentales.

2.1.3 Pregunta 3. ¿Dónde se almacenan los datos personales?

Cada soporte documental identificado puede estar almacenado en una o más ubicaciones. La respuesta a esta pregunta debe ser un listado de los lugares, gabinetes, archiveros, carpetas, computadoras, o lo que corresponda, donde se almacenen los medios identificados en la Pregunta 2.

Caso práctico

¿Dónde almacena la institución "X" los datos personales?

Una vez que la Institución "X" ha identificado los soportes documentales y los soportes documentales de almacenamiento, realiza un listado de los sitios y medios donde dichos soportes, son guardados o utilizados. De esta manera, comienza por identificar, de lo general a lo particular, los sitios y medios como oficinas, computadoras o archiveros, y después va identificando los contenedores más específicos, en la tabla que se muestra a continuación:

Sitios de resguardo	¿Qué medios de almacenamiento se resguardan?
Señalar todos los sitios, ya sean físicos o digitales donde se encuentran los medios de almacenamiento. **Oficinas de la Institución**	*Indicar todos los medios de almacenamiento usados.* Cajones de escritorio Estantes/Archiveros Dispositivos móviles (laptops, teléfonos inteligentes) Memorias USB, discos duros extraíbles y otros medios de almacenamiento digital
Medios de almacenamiento físico	**¿Qué soportes documentales o medios de almacenamiento físico se resguardan?**
Indicar todos los medios de almacenamiento físico referidos en el apartado anterior. **Cajones de escritorio**	*Indicar los soportes documentales o los medios en los que se resguardan los datos.* Expedientes en trámite, memorias USB, CD´s y DVD´s.
Estantes/Archiveros	Soportes documentales impresos que se entregan al aspirante, impresiones de las cartas de aceptación, impresiones de expedientes
Medios de almacenamiento digital	**¿Qué soportes documentales, formatos o medios de almacenamiento digital se resguardan?**
Señalar todos los medios de almacenamiento digital referidos. **Computadoras de escritorio**	*Indicar el o los soportes documentales en los que se resguardan los datos.* Correo y carpetas de almacenamiento de las cuentas de correo de los empleados involucrados en el programa de servicio social, archivo serviciosocial.xls, documentos tipo: nombre_prestador.pdf o nombre_prestador.doc, videos de vigilancia en las oficinas.

Medios de almacenamiento digital	¿Qué soportes documentales de almacenamiento digital se resguardan?
Computadoras portátiles (Laptop)	El cliente de correo y las carpetas de almacenamiento de las cuentas de correo de los empleados involucrados en el programa de servicio social, archivo serviciosocial.xls, documentos tipo: nombre_prestador.pdf o nombre_prestador.doc, videos de vigilancia en las oficinas, carpeta "Programa servicio social".
Teléfonos inteligentes, tabletas y otros dispositivos móviles	En este caso práctico, los correos y carpetas de almacenamientos de documentos en las cuentas de los empleados que tengan vinculado el correo a su celular, siempre y cuando el superior jerárquico lo autorice.
Memorias USB, discos duros extraíbles y otros medios de almacenamiento digital	*Indicar el contenido almacenado.* Uso del archivo serviciosocial.xls
Almacenamiento en línea/computo en la nube	*Se debe señalar lo que almacena en la nube.* Los correos y carpetas de almacenamiento de documentos de los empleados que operan en el proyecto.

Para llenar esta tabla, la Institución "X" consideró todas las ubicaciones donde suele trabajar y las tareas que realiza en cada lugar. De manera general, se podría identificar que almacenan diferentes medios en múltiples lugares. Según sea el caso, un mecanismo para disminuir el riesgo podría ser el reducir el número de sitios y medios utilizados para guardar información.

De igual manera, es importante considerar carpetas físicas o digitales específicas. Por ejemplo, los empleados de la Institución "X" que trabajan en el programa de servicio social podrían tener todos sus documentos digitales relacionados con los prestadores en la carpeta "Programa servicio social" de la computadora y hacer una copia de respaldo de esa carpeta en un disco duro externo, para después resguardarlo en el archivo de la Institución.

El **Anexo A.3** contiene una tabla en blanco similar a la Institución "X" para que las áreas de este Instituto elaboren sus propias listas de sitios y medios de almacenamiento.

Importante

Cómputo en la nube

El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en ingles) de Estados Unidos, define al cómputo en la nube[4], como un modelo para permitir acceso de red de forma ubicua, conveniente y bajo demanda, a un grupo compartido de recursos informáticos configurables, que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios.

En alineación con el NIST, la Ley de Datos en el artículo 2, fracción VI considera los tres modelos de servicio de cómputo en la nube, que son los siguientes:

1. **Software (Software as a Service, SaaS):** Este servicio permite al consumidor utilizar las aplicaciones del proveedor que ya se encuentran en la infraestructura en la nube. Un ejemplo, es el correo web. Cabe mencionar que al consumidor no le será posible administrar ni controlar la infraestructura (sistema operativo, almacenamiento, entre otros recursos) únicamente algunos parámetros de configuración de la aplicación.

2. **Plataforma (Platform as a Service, PaaS):** Permite hacer el despliegue de aplicaciones previamente adquiridas o creadas por el consumidor, y cuyas herramientas y/o lenguajes de programación, se encuentren soportados en la infraestructura en la nube. En este servicio el consumidor tampoco puede administrar la infraestructura, únicamente algunas configuraciones para el hosting de sus aplicaciones.

3. **Infraestructura (Infrastructure as a Service, IaaS):** Permite al consumidor tomar el control del sistema operativo, aplicaciones, procesamiento, almacenamiento, redes y otros recursos de la infraestructura para desplegar y ejecutar aplicaciones. Así como el control limitado de componentes de red específicos.

Una vez que conocemos el tipo de servicio de cómputo en la nube, podemos identificar los modelos de implementación, es decir, cómo nos será proporcionado. Para ello, el NIST detalla los que se enlistan a continuación:

a) **Nube privada:** Es aquella proporcionada únicamente para la organización. La puede administrar la misma organización, un tercero o ambos, ya sea con la infraestructura ubicada en las instalaciones de la organización (on-premise) o fuera de ella (off-premise).

b) **Nube comunitaria:** La infraestructura de la nube es compartida por diversas organizaciones usuarias y que comparten requerimientos o propósitos comunes (seguridad, políticas, misión, entre otros). La nube puede ser administrada por dichas organizaciones o por un tercero y también puede existir on-premise y off-premise.

[4] Para más información, consultar https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Dato Útil

Usando cómputo en la nube

Aunque los servicios y aplicaciones de cómputo en la nube pueden proveer altos estándares de privacidad y seguridad de la información, al igual que otros servicios y aplicaciones, su nivel de seguridad depende de los términos de uso o del contrato de servicio, así como de la configuración que defina el usuario del servicio (el área responsable), por lo que es muy recomendable atender las medidas de seguridad que se analizarán en la Etapa 2.

La Ley de Datos en el artículo 63 y 64, permite el uso de cómputo en la nube para tratamiento de datos personales, siempre y cuando el proveedor garantice políticas de protección de los datos, y que sean equivalentes a los principios y deberes establecidos en dicha ley.

Independientemente del tipo de servicio que se contrate (IaaS, SaaS o PaaS), la información residirá en la infraestructura del proveedor. Por otro lado, el artículo 111 de los Lineamientos Generales, **otorga el carácter de encargado, al proveedor de servicios de cómputo en la nube.**

En el artículo 64 de la Ley de Datos, para el uso de los servicios, el proveedor debe cumplir por lo menos con:

- Tener y aplicar políticas de protección de datos personales afines a los establecidos en dicha ley. Esto se puede verificar través de que cuente con las siguientes certificaciones: ISO/IEC 27018, ISO/IEC 27001, SOC 1, SOC 2, SOC 3 y que el aviso de privacidad contenga toda la información indicada por la LFPDPPP.
- Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.
- Abstención de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

En el mismo artículo, la ley indica que el proveedor debe contar con al menos mecanismos para:

- Informar cambios en sus políticas de privacidad o condiciones del servicio que presta.
- Permitir que el responsable limite el tipo de tratamiento de los datos personales.
- Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.
- Garantizar la supresión de datos personales cuando concluya el servicio prestado y que el responsable los haya podido recuperar.
- Impedir el acceso a los datos personales a personal que no cuenten con privilegios de acceso e informar al responsable cuando lo requiere la autoridad competente.

Bajo ese mismo tenor, el instrumento contractual debe contener al menos las cláusulas generales contenidas en los artículos 59 de la Ley de Datos y el 109 de los Lineamientos.

La Ley General de Archivos regula la provisión de los servicios de cómputo en la nube en su artículo 62 para la gestión de documentos digitales de archivo de donde resalta que debe permitir en materia de seguridad, lo siguiente:

- Establecer altos controles de seguridad y privacidad de la información, conforme a la normatividad nacional y estándares internacionales.
- Conocer la ubicación de los servidores y de la información.
- Utilizar infraestructura de uso y acceso privado, bajo el control de personal autorizado.
- Custodiar la información sensible, así como implementar políticas de seguridad.

Por tal motivo, es menester para el área responsable, conocer toda la información inherente al servicio de cómputo en la nube tanto técnica como legal para así cumplir con nuestras obligaciones de la Ley de Datos, por mencionar algunos puntos importantes:

- Definir las responsabilidades cuando existen brechas de seguridad y vulneraciones de datos personales, así como las sanciones en caso de que lleguen a ocurrir por fallas del proveedor. En caso de que el proveedor del servicio incumpla las instrucciones de tratamiento, será considerado como responsable y no como encargado y legalmente responderá como tal.
- Conocer la ubicación física del centro de datos del proveedor y estar informado si este replica la información a otro centro de datos que se encuentra en otro país.
- Los recursos (versiones de sistema operativo, capacidad de almacenamiento, entre otros) utilizados, conforme a las características del servicio contratado.
- El proveedor debe permitir que el Instituto, con carácter de responsable, verifique que cuente con medidas de seguridad físicas técnicas y administrativas establecidas y sujeción a la normatividad aplicable.

Para más información sobre el cómputo en la nube, solicita el **"Marco de referencia para la contratación de servicios de cómputo en la nube"** desarrollado por la UTyPDP.

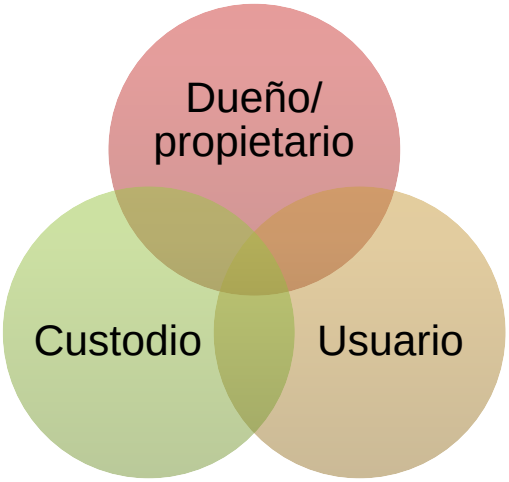
2.1.4 Pregunta 4. ¿Quién tiene permiso para acceder o manejar los datos personales?

Diversas personas en la Institución "X" pueden tener acceso a los sitios donde se almacenan los datos personales. Las personas identificadas y autorizadas para acceder a la información personal deben realizar el tratamiento con permisos específicos de uso, esto es conocido comúnmente como un esquema de privilegios.

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

Para poder conocer quienes tienen permiso para manejar o acceder a los datos personales obtenidos o recabados, es importante identificar los roles de quienes intervienen en su tratamiento.

En el tratamiento de los datos personales se identifican 3 roles:



Dueño/propietario. Es el área dueña de los datos personales, que toma decisiones respecto a su tratamiento y es el responsable final de la protección y uso de los datos.

Custodio. Es el área que implementa las medidas de seguridad de la información y asesora a los propietarios sobre los mecanismos de seguridad existentes.

Usuario. Es el área que utiliza la información.

Caso práctico

¿Quién accede o maneja los datos personales de los aspirantes y prestadores de servicio social en custodia de la institución "X"?

Con la identificación de todos los sitios y medios, la Institución "X" elabora una lista de privilegios para documentar el acceso o manejo que tienen los datos personales, en la tabla que se muestra a continuación:

Sitios de resguardo	¿Quiénes tienen privilegios de acceso?
Se deben tomar en cuenta todos los sitios de resguardo señalados en la tabla del apartado 2.1.3. **Oficinas de la Institución**	*Se deben identificar **todos** los puestos o nombres de quienes tienen permiso para acceder a los datos personales obtenidos o recabados.* Guardias de seguridad. Personal del área de recursos humanos.
Medios de almacenamiento físico	**¿Quiénes tienen privilegios de acceso?**
Cajones del Escritorio	Cada empleado tiene sus propias llaves
Estantes/Archiveros	Secretarias, asistentes
Medios de almacenamiento digital	**¿Quiénes tienen privilegios de acceso?**
Computadoras de escritorio	Cada empleado tiene su propio equipo y no se comparte con otros usuarios
Computadoras portátiles (Laptop)	El usuario de cada equipo
Teléfonos inteligentes, tabletas y otros dispositivos móviles	Los empleados que cuenten con autorización de su superior jerárquico de vincular su correo electrónico a un dispositivo móvil.
Memorias USB, discos duros extraíbles y otros medios de almacenamiento digital	Los empleados involucrados en el programa de servicio social, mismos que no podrán trasladar los medios de almacenamiento fuera de las instalaciones de la Institución, salvo autorización de su superior jerárquico.
Almacenamiento en línea/computo en la nube	El encargado del programa de servicio social y el responsable del sistema.
Soporte documental	**¿Quiénes tienen privilegios de acceso?**
Documentos tipo nombre_prestador.doc	Empleado al que se le asigne el expediente, así como su superior jerárquico.

Para los privilegios de acceso la Institución X no sólo enlista los sitios que tiene identificados, sino aquellos medios de almacenamiento y soportes documentales que deban tener un acceso restringido.

Por ejemplo, los empleados involucrados en el programa de servicio social tienen acceso al archivo digital donde se concentra el escaneo de los archivos individualizados de los prestadores de servicio social (nombre_prestador.pdf), estos deben estar restringidos y solo pueden ser vistos y modificados por el empleado al que se le haya asignado, por lo que se restringe el acceso a los demás empleados.

La idea detrás de revisar los privilegios es identificar quienes tienen acceso a los datos y controlar su tratamiento.

Los **Anexos A.2. y A.3**. proporcionan tablas en blanco similares para que el personal del Instituto elabore sus propias listas de privilegios de acceso.

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

Caso practico

La Institución "X" revisa los datos personales que maneja una vez más

Al revisar por segunda ocasión sus archivos, la Institución "X" se percató que también tiene en su poder los expedientes de aspirantes de servicio social que no fueron aceptados en el programa, por lo que deberá protegerlos de la misma forma en que cuide los de los prestadores de servicio social, en el entendido de que solamente se resguardan para cumplir con las regulaciones vigentes y que no son utilizados para ningún otro fin.

Por otro lado, la Institución notó que algunos prospectos que proporcionaron sus datos de identificación, y académicos en una feria de servicio realizada en una universidad, no firmaron el aviso de privacidad utilizado para otorgarle el consentimiento expreso a la Institución para utilizar sus datos. Por lo que tendrá que contactarlos para poner a su disposición el aviso y solicitarles su consentimiento expreso. Después de esto, deberá destruir aquellos datos de los titulares que hayan decidido no dar su consentimiento.

Resumen de la Etapa 1

¿Qué ha hecho la Institución "X" hasta este momento?

La Institución en esta etapa logró identificar y documentar:

1. Los tipos de datos que utiliza, con lo que podrá evitar el uso de los datos innecesarios.
2. Los medios y soportes documentales en los que recaba y almacena los datos personales.
3. Los sitios donde resguarda los datos personales.
4. Los privilegios de acceso/uso a los sitios, medios y soportes documentales de almacenamiento.

2.2 Etapa 2. Evaluación de las medidas de seguridad básicas

La Ley de Datos define las medidas de seguridad en su artículo 3 párrafo XX, como el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales. En otras palabras, las medidas de seguridad son elementos de control que tienen el objetivo de garantizar la seguridad de la información y se implementan en todo el ciclo de vida de los datos personales, de acuerdo con el deber de seguridad.

El artículo 33 de la Ley de Datos, enlista diversas acciones para la implementación y el mantenimiento de las medidas de seguridad para la protección de datos personales. En este sentido, se busca evitar que los datos personales sean expuestos, alterados o bloqueados por personas o entidades no autorizadas.

Importante

Entornos de trabajo

Las actividades de la Institución "X" pueden desarrollarse en ambientes físicos y digitales, así que, para esta sección, debemos considerar las siguientes definiciones:

- **Entorno de trabajo físico:** Cualquier lugar físico donde se desarrollen actividades de la Institución "X", por ejemplo, las oficinas de la Institución "X", una mesita en un café público, la oficina de un proveedor, una universidad con la que tenga un convenio, entre otros.

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

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

Las medidas de seguridad se clasifican en tres tipos:

Administrativas	Físicas	Técnicas
•Acciones para protección de la información relacionadas con gente y procesos.	•Acciones para asegurar el entorno físico de la información.	•Acciones apoyadas en la tecnología

A) Medidas de seguridad basadas en la cultura del personal, conocidas como **medidas de seguridad administrativas.** Se encuentran enfocadas en roles y responsabilidades de personas o entidades involucradas en el tratamiento de los datos personales.

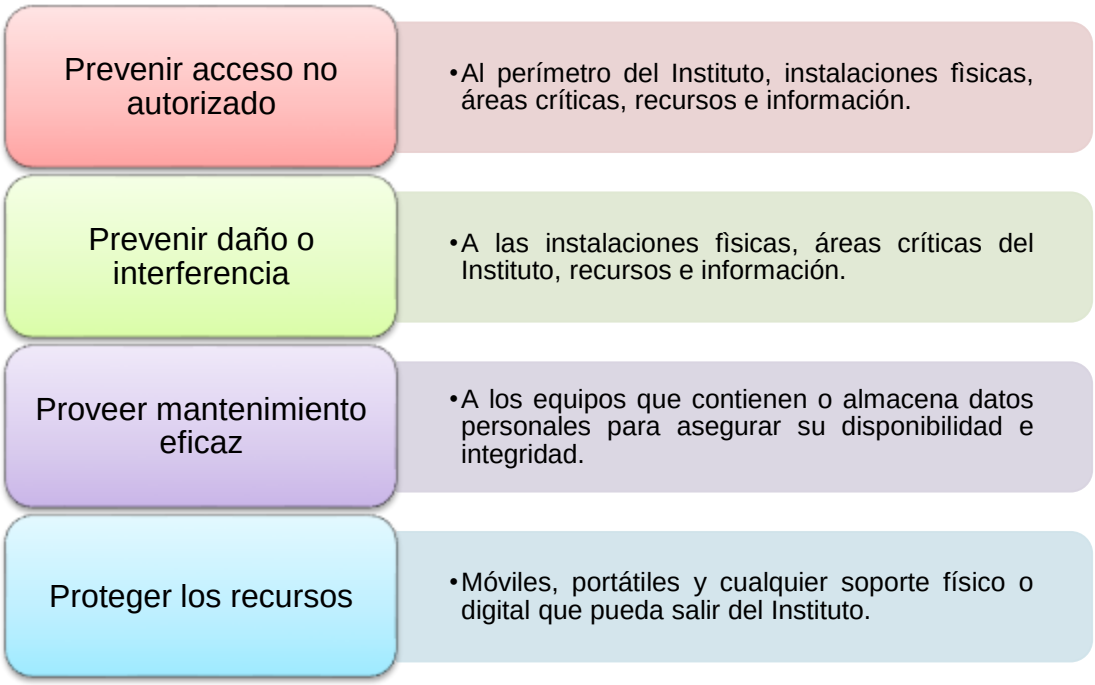
La ley define estas medidas como:

- Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.
- La identificación, clasificación y borrado seguro de la información.
- Sensibilización y capacitación del personal, en materia de protección de datos personales.

Dentro de las medidas administrativas podríamos encontrar los siguientes ejemplos:

- Concientización del personal en seguridad de la información y protección de datos personales,
- Políticas de escritorio limpio,
- Bloqueo de pantalla del equipo,
- Sanciones

B) Medidas de seguridad en el entorno de trabajo físico, conocidas como **medidas de seguridad físicas.** La Ley de Datos considera la protección del entorno físico de los datos personales y de los recursos involucrados en su tratamiento y recomienda considerar lo siguiente:



En este caso podrían ser candados, CCTV, bitácoras de entrada y salida de personal y visitantes, entre otros más, según corresponda al proceso y actividades del personal en el área, así como la efectividad de la medida.

En el caso del mantenimiento eficaz, busca asegurar en los equipos, la disponibilidad y la confidencialidad de los datos personales, es decir, que siempre se pueda acceder a ellos y que sólo sean modificados por aquellos que han sido autorizados.

C) Medidas de seguridad en el entorno de trabajo digital, conocidas como **medidas de seguridad técnicas.** La Ley de Datos considera todas las acciones y mecanismos tecnológicos relacionados con software y hardware para proteger el entorno digital de los datos personales y de los recursos involucrados en su tratamiento. Para ello recomienda considerar al menos lo siguiente:

- Que el acceso a las bases de datos, información y recursos sea para usuarios identificados y autorizados.
- Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones.

- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware.
- Gestión de las comunicaciones, operaciones y medios de almacenamiento de los recursos informático en el tratamiento de datos personales.

Importante

Estándares internacionales de la ISO

La Organización Internacional de Estandarización (por sus siglas en inglés, ISO), es una organización independiente y no gubernamental, conformada por 164 países miembros, con sede en Génova, Suiza. Desde su fundación en 1947, ha desarrollado y publicado más de 23,000 estándares de diversos temas como seguridad alimenticia, tecnología, manufactura.

Los estándares de la ISO son desarrollados a través de un proceso de consenso y por expertos de todo el mundo con la finalidad de que reflejen la riqueza del conocimiento y experiencia internacional de los miembros. El uso de estándares permite la optimización del uso de recursos, asegurar que los productos y servicios son seguros, confiables y de buena calidad.

En el caso de estándares de seguridad, ISO/IEC 27000 es la familia de estándares para seguridad de la información. Éstos ayudan a establecer y mantener acciones de gobierno de seguridad de la información, conocidas como estratégicas y acciones tácticas, correspondientes a la gestión de la seguridad.

Los estándares para gestión permiten: clasificar la información, realizar análisis de riesgos, seleccionar controles o medidas de seguridad, monitorear el desempeño de los controles y auditar los sistemas de gestión.

En particular, **el estándar ISO/IEC 27002:2013,** provee las pautas para seleccionar, implementar y administrar controles que consideren los ambientes de riesgos de seguridad de información de una organización. Por tal motivo, se sugiere tomar como referencia obligada para las medidas de seguridad técnicas, físicas y administrativas. Cabe mencionar que es el estándar más utilizado por su diseño como referencia en selección de controles en la implementación de un sistema de gestión de seguridad de la información.

A partir de la sección 2.2.1, se detallan algunos ejemplos de medidas de seguridad administrativas, físicas y técnicas fundamentadas en el ISO/IEC 27002:2013[5]. Para auxiliar

[5] https://www.iso.org/standard/54533.html

en la determinación de las medidas de seguridad físicas, técnicas y administrativas que podrías implementar, se sugiere la consulta del estándar mencionado, así como el NIST SP 800-53[6], COBIT[7] que te servirán como guías.

Durante la evaluación de las medidas de seguridad, los responsables y encargados del tratamiento de datos personales deberán contestar Sí, No o No aplica, a las preguntas de la sección, dependiendo de los medios y sitios identificados en la Etapa 1.

2.2.1 Medidas de seguridad Administrativas

Una de las principales causas por las que ocurre robo o extravío de datos personales, e incluso de cualquier información relevante para las instituciones, es simplemente porque los datos no se protegen adecuadamente.

El siguiente grupo de preguntas tienen como objetivo identificar algunas de las prácticas inadecuadas más comunes, que podrían provocar una vulneración a la seguridad.

Medidas de seguridad administrativas	**A.1 ¿Evitas dejar a la vista información personal y llevas registro de su manejo?**
	A.2 ¿Tienes mecanismos para eliminar de manera segura la información?
	A.3 ¿Has establecido y documentado los compromisos respecto a la protección de datos?

En los siguientes apartados encontrarás algunos ejemplos de controles aplicables a las medidas de seguridad administrativas ejemplificadas con las preguntas anteriores.

[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[7] https://www.isaca.org/resources/cobit

A.1. ¿Evitas dejar a la vista información personal y llevas registro de su manejo?

Cuando se dejan datos personales sin supervisión o a la vista, corren el riesgo de que sean sustraídos por alguien más (ya sea interno o externo a la Institución). Por ello, es importante considerar controles como los siguientes ejemplos:

Ejemplo de control	Descripción
A.1.1. Política de escritorio limpio	No dejar a simple vista documentos importantes, llaves, identificaciones, bloquear el equipo de cómputo cuando no esté frente a él, no anotar contraseñas en "post-it", entre otros.
A.1.2. Hábitos de cierre y resguardo	Esto debe incluir conductas como: que cada empleado cierre sus cajones, que las cosas importantes siempre se mantengan bajo llave si no están en uso y/o que el último en salir de las oficinas cierre los archiveros y las puertas con llave, y active las alarmas.
A.1.3. Impresoras, escáneres, copiadoras y buzones limpios	Nunca se deben dejar abandonados documentos en áreas de uso común como las mencionadas, mucho menos aquellos que contengan datos personales o información clasificada.
A.1.4. Gestión de bitácoras, usuarios y acceso	Para controlar el acceso a los sitios, medios de almacenamiento, soportes documentales y equipo de cómputo, se puede hacer a través del uso de bitácoras, tan simples como una lista donde se anote la fecha, hora, nombre de la persona que accede a un archivero para consultar un expediente, o bien, llevar bitácoras automatizadas. Es importante habilitar los mecanismos de registro en los equipos de cómputo y su software para identificar la actividad de los usuarios, así como revisar que las credenciales y permisos de los usuarios estén bien definidos.

A.2. ¿Tienes mecanismos para eliminar de manera segura la información? [8]

Una fuga de información puede ocurrir al desechar documentos en la basura sin darle importancia a la información que contiene ya que puede ser recuperado y visto por cualquier persona.

En los medios digitales, una vez que se desecha el medio digital, por ejemplo, una memoria USB o un disco duro, la información puede ser recuperada con ciertas herramientas y técnicas especializadas incluso aunque esté roto. Por ello se deben tomar en cuenta controles como:

Ejemplo de control	Descripción
A.2.1 Destrucción segura de documentos	Los documentos y otros medios físicos se deben destruir antes de ser desechados, por ejemplo, con triturado o incinerado. Cuando se adquiere equipo para estas tareas se debe evaluar que tan difícil sería para una persona recuperar la información, por ejemplo, hay trituradoras que hacen tiras el papel y otras que lo hacen pequeños trozos. Con tiempo y esfuerzo es posible recuperar un documento hecho tiras, pero es muy difícil recuperar uno hecho "confeti" o cenizas. Otra opción es almacenar en un sitio seguro los documentos a triturar y entregarlos periódicamente a alguien que preste el servicio de destrucción de documentos, sin olvidar que debe existir un contrato que estipule claramente el deber de confidencialidad del prestador de servicio. Lo anterior, considerando el cuadro de clasificación archivística de la Institución o periodos de retención.
A.2.2 Destrucción segura de la información en equipo de cómputo y	Cuando en los equipos de cómputo se borra o elimina información con un clic, únicamente deja de ser fácilmente accesible para el usuario- pero sigue en el disco duro hasta que nueva información la "sobrescribe".

[8] El Instituto cuenta con los Procedimientos y plazos de conservación para el bloqueo en su caso y supresión de los datos personales que obran en posesión del Instituto Nacional Electoral. Disponibles en: https://norma.ine.mx/unidades-tecnicas/unidad-tecnica-de-transparencia-y-proteccion-de-datos-personales/vigente/no-normativo/procedimientos-y/o-procesos.

medios de almacenamiento digital	Por lo anterior, existen herramientas de software que borran de "forma segura" archivos digitales específicos o dispositivos de almacenamiento completos. Cuando la vida útil de un equipo de cómputo o medio de almacenamiento digitales ha terminado, es recomendable destruirlo físicamente y asegurarse de que la información no sea recuperable para así evitar posibles fugas de información. Esto lo puede hacer la misma Institución o contratar a un tercero para este servicio, cuando la cantidad de equipo de cómputo es mayor.
A.2.3 Fijar periodos de retención y destrucción de información	Es importante identificar de manera regular toda la información que ya no es de utilidad y que no requiere almacenarse para cumplir con alguna responsabilidad legal o contractual. Los procedimientos de eliminación de información de gran valor o a gran escala deben ser formales y estar registrados en bitácoras. A su vez es importante considerar el límite de periodos de retención que se requieran y destruirla adecuadamente.
A.2.4 Tomar precauciones con los procedimientos de re-utilización	Por diversas razones, el Instituto puede optar por diferentes mecanismos de reciclado para minimizar costos, pero se debe prevenir la exposición de datos personales. Por ejemplo, en el uso de "bandejas de papel reciclado", no deben dejar hojas de documentos con datos personales. Cuando el equipo de cómputo tenga que cambiar de dueño, por ejemplo, de un empleado a otro, es importante respaldar la información relevante para el Instituto y borrar de manera segura los datos que resguarda el equipo.

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

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

Ejemplo de Control	Descripción
A.3.1. Informar al personal sobre sus deberes mínimos de seguridad y protección de datos	El personal involucrado en el tratamiento de datos personales debe estar informado de manera explícita que tiene un compromiso y responsabilidad sobre la información en su custodia, y con las tareas específicas a realizar. Por ejemplo, informar al personal de nuevo ingreso sobre sus funciones y obligaciones para la protección de datos e incluir cláusulas muy específicas al respecto cuando se hace una contratación. Así como informar a los empleados de las posibles consecuencias y medidas disciplinarias relacionadas, en caso de no cumplir con sus deberes.
A.3.2. Fomentar la cultura de la seguridad de la información	Es necesario inculcar la seguridad de la información como una práctica cotidiana, recordando la importancia de este deber e incentivando a los empleados para que entre ellos se recuerden el uso de medidas de seguridad y buenos hábitos de tratamiento de los datos.
A.3.3 Difundir noticias en temas de seguridad	Es importante hacer difusión de noticias en temas de seguridad ya que es una forma de demostrar que cualquiera puede ser susceptible de ataques y así estén conscientes de lo que podría ocurrir ante un descuido de las medidas de seguridad implementadas en la Institución.
A.3.3. Prevenir al personal sobre la Ingeniería Social	El ser humano es considerado como el eslabón más débil en el ámbito de la seguridad. De manera general, se considera a la ingeniería social como un conjunto de técnicas para influenciar a una persona a realizar acciones que pueden estar o no dentro de sus intereses o responsabilidades. Estas técnicas pueden ser utilizadas por criminales para

	engañar a personas desprevenidas en línea, por teléfono o personalmente. Se debe invitar a los empleados a cuestionar en todo momento si alguna solicitud a través de correo, llamada o de forma verbal, tiene sentido y si está dentro de sus responsabilidades cumplirla, de lo contrario negarse educadamente a entregar la información o a realizar la acción solicitada e informar de este hecho a su jefe inmediato.
A.3.4. Asegurar la protección de datos personales en subcontrataciones	Ninguna institución debe asumir que un proveedor o cualquier externo tomará las medidas de seguridad necesarias para proteger la información personal y que la tratará como confidencial, sin que esto se manifieste explícitamente. A través de cláusulas que especifiquen claramente el tratamiento legítimo y las medidas de seguridad implementadas para la protección de los datos personales, se podría asegurar que un proveedor o encargado tomen medidas e incluso a través de supervisiones para revisar que estén cumpliendo con ello. Otros tipos de convenios que deben revisarse son los relacionados a la compra, venta o intercambio de datos de titulares, revisando a detalle que los datos sean utilizados con el consentimiento del titular. Además, en el uso de servicios de almacenamiento en línea o de cómputo en la nube, se debe revisar y evaluar si el contrato o instrumento legal, garantiza seguridad y confidencialidad de los datos que se almacenen.

La ley platicada

Acciones para la seguridad

Los Lineamientos establecen en el artículo 66 que el responsable de los datos personales debe dar aviso al titular y al órgano garante de las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto se confirme que ocurrió una vulneración y haya tomado acciones para reducir la posible afectación de los titulares. La notificación a los titulares debe de considerar al menos:

1. La naturaleza del incidente o vulneración ocurrida.
2. Los datos personales comprometidos.
3. Recomendaciones dirigidads al titular para proteger sus intereses.
4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde pueden obtener más información al respecto.
6. La descripción de las circunstancias generales en torno a la vulneración.
7. Cualquier información o documentación conveniente para apoyar al titular.

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

Para las Instituciones, incluso para aquéllas con gran madurez en el tema de seguridad de la información, las vulneraciones a la seguridad de los datos personales pueden resultar particularmente complicado. Deben contar con procedimientos que disminuyan la posible afectación a los titulares de los datos personales y a la Institución. Por ello, se requiere tomar medidas como:

Ejemplo de control	Descripción
A.4.1. Tener un procedimiento de notificación	Ante un evento o un incidente de seguridad, debe tener muy claro a quién debe avisar en la Institución. Por ello, debe establecerse un plan de respuesta a incidentes o atención de vulneraciones dentro de la Institución en caso de que ocurra.

	El responsable debe evaluar la información afectada y tener los medios para notificar a los titulares de lo ocurrido, esto con el fin de alertarlos y que tomen precauciones. A su vez, debe evaluar el posible impacto a las operaciones y tomar acciones que mitiguen el incidente, por ejemplo, actualizando sus procedimientos y medidas de seguridad, dependiendo de las afectaciones del incidente.
A.4.2. Realizar revisiones y auditorías	Se debe considerar la revisión periódica a la Institución por un especialista en temas de seguridad de la información para que realice evaluaciones y recomendaciones. Este tipo de revisiones podrían ayudar a revelar malas prácticas en el tratamiento de datos personales o la existencia de vulneraciones a la seguridad no detectadas, por ejemplo, a través de pruebas de penetración o pentest. A partir de los resultados de las revisiones y auditorías que se hagan, el responsable debe tomar medidas para actuar ante las áreas de oportunidad e informarlas a los involucrados en el tratamiento de datos personales.

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

Si se realizan respaldos de la información importante periódicamente, es posible mitigar las consecuencias de incidentes como daño de manera parcial o total debido a fallas en los sistemas o aplicaciones, por errores de operación de las personas, o bien por interrupciones de energía eléctrica. Por ello, se describen ejemplos de controles:

Ejemplo de control	Descripción
A.5.1 Respaldo en soportes documentales digitales	En la medida de lo posible se deben almacenar los documentos físicos en medios digitales, es decir, capturar, digitalizar o escanear la información en papel para almacenarla, de forma tal que se resguarde el mínimo de información en papel y sólo se imprima cuando sea estrictamente necesario. Es más práctico respaldar información copiando un archivo de un medio digital a otro, comparado con

	fotocopiar, organizar y almacenar documentos en papel para respaldar periódicamente.
A.5.2 Periodicidad de respaldos	Es importante que los respaldos se realicen de manera regular y también cada vez que haya una actualización importante de los datos en posesión del Instituto. Se recomienda realizar respaldos parciales de la información crítica, diaria o semanalmente y respaldos de toda la información, cada quince días o mensualmente.
A.5.3 Resguardo de respaldo fuera de las instalaciones	Es importante que los respaldos no se encuentren en la misma ubicación física que la información que se está respaldando y hacer pruebas de recuperación de las copias de respaldo para asegurarnos que la información se encuentra íntegra, así como para probar que ante una contingencia, podemos utilizar a los respaldos realizados.

Dato útil

Protegiendo la información

La información se puede encontrar en distintos soportes documentales, ya sea escrita, gráfica, impresa, de forma digital, en audio y otros soportes. Sin importar el tipo de soporte documental, debe protegerse. Por ello, la seguridad de la información cubre principalmente las tres propiedades que se describen a continuación:

1. La confidencialidad, busca proteger la información de ser robada o expuesta.
2. La integridad, busca protegerla ante alteraciones, daños o eliminado intencional o accidental.
3. La disponibilidad busca evitar que la información sea secuestrada o denegada.

La información puede ser robada cuando no existe un control de acceso al área donde se almacena, por ejemplo, al estar en archiveros sin chapa y si no se cuenta con mecanismos de control de acceso al área, un intruso puede entrar y extraerla. De manera similar ocurre en un centro de datos, cuando no hay controles de acceso seguro, un intruso puede entrar y robar medios de almacenamiento o dañar los equipos. La información puede ser expuesta, al tirar documentos en la basura, sin tachar la información sensible que contiene.

A falta de controles de acceso físicos a la información, esta puede ser alterada cuando alguien cambia el contenido de un documento físico o reemplazarlos por falsos. Cuando ésta se encuentra de forma digital, alguien con acceso al sistema, también podría reemplazar el archivo o documento.

De forma accidental, puede ser dañada o eliminada cuando ocurren fenómenos naturales, exposición a químicos, incidentes físicos o fallas en la infraestructura.

2.2.2 Medidas de seguridad Físicas

Conforme los equipos de cómputo son cada vez más pequeños, ligeros y convenientes se vuelve muy fácil para las personas llevar información con ellos, lo que puede resultar en que sea común revisar información en lugares públicos como un restaurante, cafetería o en el transporte público. Por otro lado, la facilidad para llevar dispositivos o equipo de cómputo a cualquier lado, puede exponerlos a que sean perdidos o robados. La seguridad del entorno de trabajo físico es un elemento básico para mitigar vulneraciones a la seguridad de los datos personales.

Con respecto a las medidas de seguridad físicas, no sólo se trata de proteger las áreas críticas del Instituto, en donde se tratan los datos personales. De manera ilustrativa, en el siguiente diagrama, se observa que la ley recomienda considerar las medidas de seguridad físicas desde el perímetro del Instituto, hasta los equipos donde se tratan los datos personales.

En los apartados siguientes se identificará con las siguientes mínimas preguntas, si tiene algunas medidas de seguridad físicas implementadas:

Medidas de seguridad físicas	**¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?**
	¿Tienes medidas de seguridad para evitar el robo?
	¿Proteges el movimiento de información en entornos de trabajo físicos?

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

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

Ejemplo de control	Descripción
B.1.1. Alerta del entorno de trabajo	No se debe permitir que alguien sin motivos relacionados al funcionamiento del área ingrese al entorno de trabajo. Se debe tener precaución con las personas no autorizadas, por ejemplo, se debe cuestionar la presencia de un extraño sin acompañamiento o que se encuentre cerca del entorno de trabajo.
B.1.2. Mantener bitácoras del personal con acceso al entorno de trabajo	En entornos como oficinas o centros de cómputo, es importante mantener un registro de todos los que ingresan y salen. Adicionalmente, el registro puede contener hora de entrada y salida, persona a la que visita, entre otros aspectos.

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

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

Ejemplo de control	Descripción
B.2.1. Cerraduras y candados	En las oficinas se debe contar como mínimo con gavetas, escritorios, o archiveros que se puedan cerrar con llave. El mismo principio aplica para laptops con candado o maletas con cierre de combinación.
B.2.2. Elementos disuasorios	Existen medidas de seguridad que reducen de manera significativa el interés de un atacante, por ejemplo, alarmas (tanto para el entorno como para los dispositivos), guardias de seguridad, rejas, maletines de seguridad, entre otros.
B.2.3. Minimizar el riesgo oportunista	Es necesario limitar el número de entornos de trabajo donde se realice tratamiento de datos personales, si es necesario trabajar constantemente en otros entornos (como aeropuertos u oficinas de otras instituciones) nunca dejar un elemento que contenga datos personales sin supervisión.

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

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

Ejemplo de control	Descripción
B.3.1. Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento digital	Se debe registrar el permiso o la acción relacionada a la salida y entrada de los elementos mencionados en una bitácora, esto con el fin de que, en caso de pérdida, robo, daño o extravío se tenga control del posible impacto
B.3.2. Mantener en movimiento sólo copias de la información, no el elemento original	Un incidente común puede ser la pérdida o extravío de información disponible. La información que sale de los entornos de trabajo usuales debería ser una copia de ella y no la información original.
B.3.3. Usar mensajería certificada	Es recomendable que el envío físico de medios que contienen datos personales se realice con mensajería segura/certificada, o en su defecto con personal de confianza, y siempre se debe solicitar y conservar el acuse de recibo del envío.

2.2.3 Medidas de seguridad técnicas

Las medidas de seguridad técnicas son aplicables en toda la infraestructura tecnológica y se clasifican generalmente en:

a) Control de acceso: Para garantizar que sólo quien está autorizado, acceda a la información y realice el tratamiento permitido. El control de acceso debe estar basado en autenticación y autorización.

b) Operación de las comunicaciones e infraestructura: Para proteger la información que se encuentra en circulación, filtrar el flujo de la información, salvaguardar la información accedida, procesada o almacenada y proteger la infraestructura.

c) Sistemas de información: Para proteger la información de accesos, modificaciones, daños o bloqueos no deseados o no autorizados. A través de verificaciones de datos de entradas de los aplicativos, detectando y filtrando posibles riesgos, metodologías de desarrollo seguro de código, análisis de vulnerabilidades o verificaciones de que el procesamiento de la información sea íntegro.

Las actividades de las Instituciones son llevadas a entornos digitales, por lo que se vuelve primordial proteger equipos de cómputo y dispositivos de almacenamiento contra el acceso no autorizado y contra amenazas informáticas como el software malicioso.

Las siguientes preguntas ayudarán a identificar algunas de las medidas de seguridad técnicas con las que debes contar:

Medidas de seguridad técnicas	**¿Realizas actualizaciones del equipo de cómputo?**
	¿Revisas periódicamente el software instalado en el equipo de cómputo?
	¿Tienes medidas de seguridad para acceder al entorno de trabajo digital?
	¿Revisas la configuración de seguridad del equipo de cómputo?
	¿Tienes medidas de seguridad para navegar en entornos digitales?
	¿Proteges el movimiento de información en entornos de trabajo digitales?

Dato útil

Malware

Malware es la abreviatura de *"Malicious software"*, un término que engloba a todo tipo de programa o código malicioso cuyas funciones pueden variar desde extraer, borrar e incluso "secuestrar" la información en equipos de cómputo o causar mal funcionamiento en los sistemas. Pese a que se suele escuchar de diversas clasificaciones de código malicioso como virus, troyanos, gusanos, entre otros, y las variantes que surgen cada día, la clasificación se hace con respecto al objetivo que busca lograr el atacante en el equipo.

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

Un equipo de cómputo puede tener vulnerabilidades que, en caso de no ser subsanadas, pueden dar lugar a instalación de programas maliciosos como *malware* o presentar fallos en el desempeño o funcionamiento del equipo.

Dentro de las vulnerabilidades, principalmente pueden ser errores de configuración del equipo, sistema operativo o software sin actualizaciones, no contar con antivirus. Para ello, se describen los siguientes ejemplos de controles:

Ejemplo de control	Descripción
C.1.1 Actualización del sistema operativo	El sistema operativo debe ser el más reciente y estable. Los fabricantes de sistemas operativos liberan constantemente actualizaciones, conocidas como "parches" para subsanar las vulnerabilidades que detectan. No es recomendable usar sistemas operativos que ya no tienen soporte del fabricante ya que el equipo queda expuesto a diversos tipos de ataques y no hay forma de protegerlos. Los fabricantes anuncian con la debida antelación el fin de soporte para que los usuarios tomen sus precauciones.
C.1.2 Actualización del software	El software utilizado, debe ser la versión más reciente o estar actualizado. La mayoría del software instalado está configurado para actualizarse de manera periódica, sin embargo, debe verificarse que efectivamente esté habilitada esta función, de lo contrario se debe programar al menos una vez al

	mes la descarga y/o instalación de las actualizaciones correspondientes.
C.1.3 Actualización del hardware	Es de vital importancia considerar el tiempo de vida que el fabricante indica para el equipo de cómputo que se adquiere o tiene. Una vez que termina el tiempo de vida estimado, el fabricante deja de elaborar los componentes y en caso de daño, será difícil encontrarlos, además de que, pasado el tiempo de vida, no existe garantía del adecuado funcionamiento del hardware.

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

Es importante revisar periódicamente los tipos de programas que se encuentran instalados en el equipo de cómputo, para verificar que se esté utilizando sólo software autorizado, así como evitar tener alguno no deseado. A continuación, se describen algunos ejemplos:

Ejemplo de control	Descripción
C.2.1 Uso de software actualizado	El uso de software actualizado evita que las posibles vulnerabilidades de versiones obsoletas o anteriores sean explotadas por un atacante.
C.2.2 Restricción de uso de software distinto al Institucional para descargar o compartir archivos	Es de especial importancia evitar el uso de software para descargar o compartir archivos en equipos de cómputo del Instituto, o con otros dispositivos personales, como tabletas o celulares, no sólo para evitar infringir la ley de derechos de autor, sino porque este tipo de software podría dar acceso a ciberdelincuentes a la información del equipo. Tampoco se recomienda utilizar navegadores distintos a los que instala la Institución pues podrían dar acceso a posibles atacantes.
C.2.3 Verificación de licencias	Se debe verificar que no se tenga instalado software sin licencia o “pirata”, ya que éste podría estar infectado con *malware* o simplemente no operar como el original y causar pérdida de información o daño en el equipo.

Dato útil

BYOD, BYOC, BYO

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

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

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

Por ejemplo, algunos empleados de la Institución "X" tienen su cuenta de correo institucional, enlazada a un *smartphone*, sólo para asuntos laborales. Para recibir mensajes personales usa otra cuenta de correo y aunque en su laptop realiza operaciones personales, lo hace con un usuario diferente.

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

El equipo de cómputo es susceptible a que cualquiera lo pueda utilizar, incluso personal no autorizado. Las medidas de seguridad pueden evitar el uso de equipo de cómputo, medios de almacenamiento o acceso a un entorno de trabajo digital sin autorización, por ejemplo, mediante el uso de contraseñas o cifrado, o de aplicaciones o dispositivos para la verificación de identidad del usuario.

Dato útil

Cifrado y contraseñas

La mayoría de las personas están familiarizadas con el concepto de contraseña, ya sea para el uso de información secreta, o tener acceso a un equipo de cómputo, archivo o servicio. Sin embargo; la noción de contraseña puede estar ligada a un mecanismo de seguridad de la información más potente, el cifrado, que es un proceso que, a través de cálculos matemáticos, convierte la información a un formato ilegible y no accesible para todo aquél que no posea la contraseña para descifrarla.

Por ejemplo, si alguien roba un *smartphone* que tiene configurado el desbloqueo de pantalla con contraseña, no podría ver la información en ese momento sin la contraseña, pero podría conectarlo a una computadora que lo reconocería como un dispositivo de almacenamiento para ver la información almacenada. Si la víctima hubiese habilitado el cifrado del *smartphone* con una contraseña robusta previamente, el ladrón no podría ver la información y sería ilegible sin la contraseña.

Actualmente, los equipos de cómputo cuentan con algún elemento en su configuración que permite cifrar su contenido. Además, existe software que permite el cifrado de archivos o dispositivos de almacenamiento (como memorias USB o discos duros).

¿Cómo crear una contraseña robusta?

Una contraseña débil es susceptible a ser “crakeada” es decir, averiguar la contraseña con herramientas de software o simplemente adivinando. Por ello, se recomienda evitar el uso de información personal, fechas, nombres o palabras simples en una contraseña, así como orden numérico ascendente o descendente.

Para crear una contraseña fuerte o robusta, además de tener una frase o idea completa, es recomendable que cuente con los siguientes elementos:

- **Longitud mayor a 12 caracteres.** Una contraseña larga aumenta el tiempo en que esta pudiera ser “crackeada” en comparación con una contraseña corta, por ejemplo, es más fácil adivinar la contraseña “nubecita” que la contraseña “QO5Ngl1mas31&”.

- **Uso de mayúsculas y minúsculas.** Es preferible que una contraseña esté conformada por la combinación de estas, pues de lo contrario, el esfuerzo estaría enfocado en encontrar únicamente la palabra y no la combinación de mayúsculas y minúsculas.

- **Uso de números.** El uso de números debe evitar que sean secuencias como 123456 o descendente, ya que es probable que sean encontradas rápidamente.

- **Uso de caracteres especiales**. Hacer uso de estos, permite aumentar la complejidad de la contraseña.

Nota: Evitar usar nombres de familiares, conocidos o mascotas, sobrenombres, fechas de nacimiento, CURP y otros datos personales

Ejemplo: A la frase “megustacomerpizza”, se le agregan números, mayúsculas, minúsculas y caracteres especiales, quedando de la siguiente manera: “Megu$tacomErP1zz@.28”.

Combinando los cuatro elementos anteriores, nos dará como resultado una contraseña robusta y al usar una frase o idea completa, se puede recordar fácilmente. Puede ser difícil memorizar diversas contraseñas, una opción para esto es utilizar un software para gestión de contraseñas, por ejemplo, KeePass.

A continuación, se describen algunos ejemplos de controles para acceder al entorno digital:

Ejemplo de control	Descripción
C.3.1 Uso de contraseñas y/o cifrado	Toda información personal en un medio digital debería estar protegida por contraseña y/o cifrado, para así evitar el acceso no autorizado y/o posibles eventos de robo o pérdida de información.
C.3.2 Uso de contraseñas robustas	El uso de contraseñas robustas evita que sea fácilmente crackeada y conservar la integridad, disponibilidad y confidencialidad de los datos personales o información contenida en los equipos de cómputo.
C.3.3 Bloqueo y cierre de sesiones	Cuando no se utilice el equipo de cómputo se debe bloquear o cerrar la sesión de usuario. Si se dejará de utilizar por mucho tiempo, se debe optar por apagarlo. Todo inicio de sesión debe requerir el uso de una contraseña, token, u otro mecanismo de autenticación. Sin embargo, las buenas prácticas de seguridad recomiendan el uso del doble factor de autenticación (2FA). Un ejemplo de esto sería, para iniciar sesión al correo electrónico, que primero se solicitara un token y si es correcto, solicitara la contraseña del usuario. Se deben considerar mecanismos de bloqueo y borrado remoto para los dispositivos móviles, de tal forma que se pueda restringir o eliminar la información incluso cuando haya sido robado o extraviado.

C.3.4 Gestión de usuarios y accesos	En caso de que más de una persona tenga acceso al mismo servicio con el mismo usuario y contraseña, se debe suprimir esta práctica. Se debe tener una correcta administración de los usuarios, contraseñas y privilegios de acceso. Cada persona debe tener su propio usuario y contraseña, así como permisos asignados conforme la actividad que realice.

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

El equipo de cómputo, el software y en algunas ocasiones, los medios de almacenamiento digital tienen configuraciones disponibles que permiten incrementar su nivel de seguridad. Esta práctica es conocida como *hardening* o endurecimiento, y con su aplicación, es posible incrementar el nivel de seguridad significativamente. Por ejemplo, los siguientes controles:

Ejemplo de control	Descripción
C.4.1 *Hardening* o endurecimiento de los equipos	Se deben habilitar las opciones de seguridad que permita a sus equipos estar más seguros, por ejemplo, activar el firewall o habilitar las actualizaciones automáticas del antivirus. Es conveniente que todos los equipos del Instituto ya sean fijos o portátiles, mantengan un mismo nivel de configuración de seguridad.
C.4.2 Desactivación de configuración por default	Es de vital importancia desactivar todas aquellas configuraciones que al instalar un software se hacen por defecto para así evitar huecos de seguridad, así como el cambio de contraseñas del fabricante pues fácilmente pueden ser encontradas en la documentación de los equipos y cualquiera podría tener acceso a los equipos y borrar la información almacenada o alterar las configuraciones que tenga.

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

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

Ejemplo de control	Descripción
C.5.1. Uso de herramientas antimalware y de filtrado de tráfico	El software malicioso comprende diferentes tipos como virus, troyanos, gusanos, entre otros, que tienen por objetivo extraer datos de los usuarios como sus contraseñas. Por ello, se debe instalar al menos, software antivirus y habilitar el filtrado de tráfico (como un firewall).
C.5.2. Reglas de navegación segura	Sólo se deben navegar en sitios web esenciales para el negocio, evitando aquellos sitios no relacionados y mucho menos sitios de riesgo como son los de descarga de contenido que violan los derechos de autor o pornográficos. Todo el personal debe estar informado de los riesgos a los que se expone por visitar sitios web que no son relevantes para sus funciones, la descarga de contenido así como verificar que en la dirección web aparezca https y la imagen de un candado. Dependiendo de las funciones y atribuciones de los empleados, se puede optar por herramientas de cifrado de las comunicaciones como las redes virtuales privadas (VPN, Virtual Private Network).
C.5.3. Reglas para la divulgación de información	Antes de enviar información a un tercero, almacenarla en la nube, publicarla en un sitio web, o compartirla en redes sociales, se debe evaluar si esta acción no está poniendo en riesgo a titulares o a personal de la Institución.
C.5.4. Uso de conexiones seguras	Además de verificar que los protocolos de navegación sean seguros, se debe cuidar que la conexión también sea confiable. Las redes inalámbricas deben contar con contraseñas y configuración segura. Por ejemplo, evitar conectarse o configurar redes WEP o abiertas, susceptibles a que un tercero malintencionado descifre la contraseña para interceptar las comunicaciones. Evitar el uso de redes públicas, particularmente en los casos en que sea necesario llevar a cabo una transacción que implique el uso de información personal o contraseñas (por ejemplo, acceder a algún sistema de la Institución en el que se resguarden datos personales, mediante un dispositivo portátil, utilizando una red WiFi provista por un sitio público, como un aeropuerto o una cafetería). De manera general, si no se puede asegurar

	la conexión, se deberá evitar cualquier tratamiento que involucre datos personales en línea.

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

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

Ejemplo de control	Descripción
C.6.1. Validación del destinatario de una comunicación	Es común escuchar sobre fuga de información debido al envío erróneo de mensajes, correos, documentos, entre otros. Antes de enviar un mensaje se debe asegurar que el envío se realizará al destinatario correcto. Cuando se envíe un correo electrónico a varios destinatarios se debe revisar el destinatario, el método de envío y designación ya sea CC o con copia, CCO o con copia oculta.
C.6.2. Envío seguro de información	Al enviar información importante a través de correo electrónico, no se debe incluir en el cuerpo del mensaje, sino en un archivo individual protegido por contraseña/cifrado. La contraseña no debe estar contenida en el cuerpo del mensaje del que se envía la información, sino en un mensaje distinto o comunicarse por otro medio. Cuando se recibe información en un correo electrónico, se debe tener cuidado con los archivos y ligas adjuntas, por ejemplo, un correo de un proveedor que pide revisar una cotización no solicitada abriendo un archivo adjunto o dando clic a una liga específica. En tal caso, hay que verificar a través de un medio distinto, es decir, con una llamada telefónica al proveedor.

Importante

Análisis de Brecha

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

En este sentido, la Ley en su artículo 33, fracción V, establece la obligación que tiene el responsable de realizar un análisis de brecha, en tanto en los Lineamientos en su artículo 66 señala que en el análisis se debe considerar:

- Las medidas existentes y efectivas;
- Las medidas de seguridad faltantes, y
- La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

El resultado del análisis de brecha permite conocer el estado actual y el estado deseado o esperado.

Como se mencionó anteriormente, el estándar ISO/IEC 27002:2013 es el más utilizado para las medidas de seguridad. Se encuentra conformado por la descripción de 114 medidas de seguridad, que se agrupan en 35 categorías y 13 dominios relacionados con las siguientes familias:

1. Políticas de seguridad de la información.
2. Organización de la seguridad de la información.
3. Seguridad relativa a los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía.
7. Seguridad física y del entorno.
8. Seguridad de las operaciones.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento de sistemas de información.
11. Relación con proveedores.
12. Gestión de incidentes de seguridad de la información.
13. Aspectos de seguridad de la información para la gestión de la continuidad del negocio.
14. Cumplimiento.

Caso práctico: La Institución "X" realiza su Análisis de Brecha

Para responder las preguntas planteadas en la Etapa 2 la Institución "X" llenó una tabla que sólo para fines prácticos, se ilustra una parte de ella a continuación:

Análisis de brecha de la Institución (Medidas de seguridad existentes vs medidas de seguridad faltantes)				
Código	**Pregunta de control**	**¿Existe?**		**Justificación**
		Sí	**No**	
A. Medidas de seguridad basadas en la cultura del personal - Medidas Administrativas -				
A.1	¿Evitas dejar a la vista información personal y llevas registro de su manejo?			Parcialmente
A.1.1	Política de escritorio limpio		x	Parcialmente
A.1.2	Hábitos de cierre y resguardo	x		
A.1.3	Impresoras, escáneres, copiadoras y buzones limpios		x	
A.1.4	Gestión de bitácoras, usuarios y acceso		x	
A.2	¿Tienes mecanismos para eliminar de manera segura la información?			Parcialmente
A.2.1	Destrucción segura de documentos	x		
A.2.2	Destrucción segura de la información en equipo de cómputo y medios de almacenamiento digital		x	
A.2.3	Fijar periodos de retención y destrucción de información		x	
A.2.4	Tomar precauciones con los procesos de reutilización	x		
A.3	¿Has establecido y documentados los compromisos respecto a la protección de datos?			No

A.3.1	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos		x	
A.3.2	Fomentar la cultura de la seguridad de la información		x	
A.3.3	Difundir noticias en temas de seguridad		x	
A.3.4	Prevenir al personal sobre la Ingeniería Social		x	
A.3.5	Asegurar la protección de datos personales en subcontrataciones		x	
A.4	¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos?			No
A.4.1	Tener un procedimiento de actuación y notificación		x	
A.4.2	Realizar revisiones y auditorias		x	
A.5	¿Realizas respaldos periódicos de los datos personales?			No
A.5.1	Respaldo en soportes documentales digitales		x	
A.5.2	Periodicidad de respaldos		x	
A.5.3	Resguardo de respaldo fuera de las instalaciones		x	
B. Medidas de seguridad en entorno de trabajo físico -Medidas de seguridad Físicas -				
B.1	¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?			Si
B.1.1	Alerta del entorno de trabajo	x		
B.1.2	Mantener bitácoras del personal con acceso al entorno de trabajo	x		
B.2	¿Tienes medidas de seguridad para evitar el robo?			parcialmente
B.2.1	Cerraduras y candados	x		
B.2.2	Elementos disuasorios	x		
B.2.3	Minimizar el riesgo oportunista		x	
B.3	¿Proteges el movimiento de información en entornos de trabajo físicos?			Si

B.3.1	Aprobación de salida de documentos equipo de cómputo y/o medios de almacenamiento digital	x		Autorización la otorga el superior jerárquico.
B.3.2	Mantener en movimiento solo copias de la información, no el elemento original	x		
B.3.3	Usar mensajería certificada	x		
C. Medidas de seguridad en el entorno de trabajo digital - Medidas de seguridad Técnicas -				
C.1	¿Realizas actualizaciones del equipo de cómputo?			Parcialmente
C.1.1	Actualización del sistema operativo	x		
C.1.2	Actualización del software		x	
C.1.3	Actualización del hardware	x		
C.2	¿Revisas periódicamente el software instalado en el equipo de cómputo?			No
C.2.1	Uso de software actualizado		x	
C.2.2	Restricción de uso de software distinto al Institucional para descargar o compartir archivos		x	
C.2.3	Verificación de licencias		x	
C.3	¿Tienes medidas de seguridad para acceder al entorno de trabajo digital?			Parcialmente
C.3.1	Uso de contraseña y/o cifrado	x		
C.3.2	Uso de contraseñas robustas		x	
C.3.3	Bloqueo y cierre de sesiones	x		
C.3.4	Gestión de usuarios y accesos	x		
C.4	¿Revisas la configuración de seguridad del equipo de cómputo?			No
C.4.1	Hardening o endurecimiento de los equipos		x	
C.4.2	Desactivación de la configuración por default		x	
C.5	¿Tienes medidas de seguridad para navegar en entornos digitales?			Parcialmente

C.5.1	Instalar herramientas antimalware y de filtrado de trafico	x		
C.5.2	Reglas de navegación segura		x	
C.5.3	Reglas para la divulgación de información		x	
C.5.4	Uso de conexiones seguras		X	
C.6	¿Proteges el movimiento de la información en entornos de trabajo digitales?			Parcialmente
C.6.1	Validación del destinatario de una comunicación		x	
C.6.2	Envío seguro de información	x		

En el **Anexo C,** se proporciona una tabla en blanco similar a la de la Institución "X" únicamente para ejemplificar para la elaboración de un análisis de brecha.

Importante

Herramienta para analizar brechas de seguridad de datos personales

La tabla utilizada por la Institución "X" es únicamente ilustrativa, la herramienta para analizar las brechas de seguridad de datos personales es proporcionada por la Unidad de Transparencia y se divide en dos partes:

- **Metodología de brecha:** Documento que explica que es un análisis de brecha, describe el estándar internacional ISO/IEC 27002:2013 en el cual se basa la metodología y explica el funcionamiento del analizador de brechas de seguridad de datos personales, así como la forma en la que deberán ser respondidas las preguntas que contiene.
- **Analizador de brechas de seguridad de datos personales:** Herramienta semi-automatizada que se compone de una serie de preguntas que buscan explorar la existencia y nivel de implementación de 114 medidas de seguridad basadas en el estándar ISO/IEC 27002:2013. Una vez que termina de responder las preguntas, se deben clasificar las medidas de seguridad que el área respondió que tiene implementadas actualmente.

Importante

Análisis de riesgos

El artículo 59 de los Lineamientos, señala que el responsable deberá identificar el riesgo inherente de los datos personales contemplando su ciclo de vida y los activos involucrados en su tratamiento, ya sean humanos, materiales o cualquiera que se deba considerar.

El artículo 60 de la misma ley establece que al realizar un análisis de riesgos de los datos personales tratados, se consideren:

1. Requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
2. El valor de los datos personales de acuerdo con la clasificación previamente definida y su ciclo de vida.
3. El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
4. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración.
5. Los factores previstos en el artículo 32 de la ley de datos.

El riesgo, es la probabilidad o posibilidad de que una amenaza explote una vulnerabilidad y que ocasione un daño o pérdida a una organización.

El análisis de riesgos es un proceso que ayuda a la identificación de escenarios de riesgos de los datos personales, a través de dos pasos:

1. La identificación de amenazas que pueden causar algún daño a los datos personales. Donde una amenaza puede ser una entidad o un evento que intencional o accidentalmente, pudiera afecte la confidencialidad, integridad y/o disponibilidad de los datos personales.
2. La identificación de vulnerabilidades existentes a lo largo del ciclo de vida de los datos. Las vulnerabilidades pueden tener origen tecnológico, de procedimiento o de personas.

Dependiendo de la existencia de los mecanismos implementados actualmente, será el nivel de exposición de las vulnerabilidades.

Un escenario de riesgo es la descripción de situaciones que pueden ocurrir y relacionan los componentes del riesgo.

En general, ya identificados los componentes del riesgo (amenaza, vulnerabilidad y activo), se evalúa asignando un valor cualitativo o cuantitativo a cada escenario de riesgo, estimando la probabilidad de ocurrencia y el impacto que pudiera tener.

Importante

Herramienta para analizar los riesgos de privacidad y datos personales

La Unidad de Transparencia desarrolló una metodología para analizar los riesgos de privacidad a que está expuesto el titular derivados de un tratamiento inadecuado de sus datos personales.

Se divide en dos partes:

- **Analizador de escenarios de riesgos de privacidad:** Herramienta que se compone de una serie de preguntas que buscan explorar la existencia de escenarios de riesgos. Una vez que termina de responder las preguntas, se debe identificar los escenarios y con base en ellos, ejecutar la metodología de análisis de riesgos en privacidad**.**
- **Metodología de análisis de riesgos en privacidad:** Documento que explica qué es un análisis de riesgos en privacidad. Contiene los formatos para su ejecución.

Si requieres más información acerca de este tema contacta a la Unidad de Transparencia.

Resumen de la Etapa 2

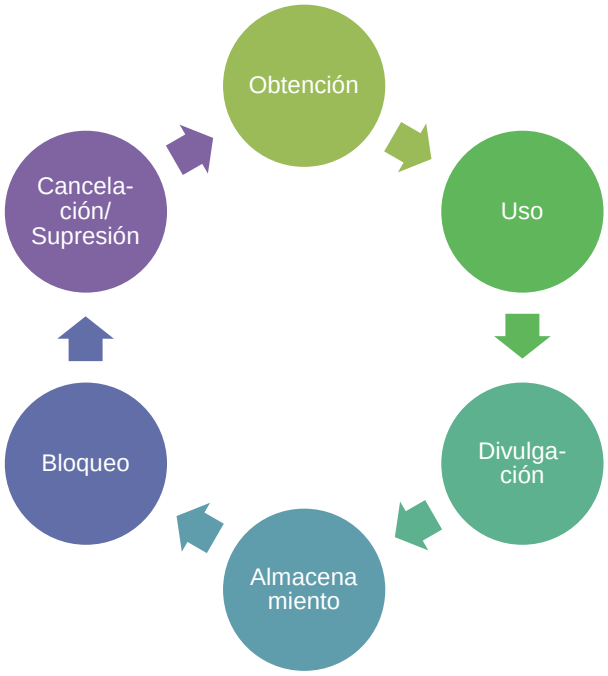
¿Qué ha hecho la Institución "X" hasta este momento?

En esta etapa, la Institución logró identificar y documentar:

- Las medidas de seguridad con las que ya cuenta, así como las que requerirá incluir en su plan de trabajo.
- Los riesgos a los que están expuestos lo datos personales .

2.3 Etapa 3. Plan de Trabajo

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



La ley platicada

Plan de trabajo

El artículo 33 de la Ley de Datos, señala la elaboración de un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

Para la elaboración del plan de trabajo, señala que se conforma de lo siguiente:

- El resultado del análisis de riesgos de datos personales, el cual incluya amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.
- El resultado del análisis de brecha y la comparación de las medidas de seguridad existentes con respecto a las medidas faltantes.

Lo anterior, permitirá establecer y mantener las medidas de seguridad que contendrá el plan de trabajo de manera detallada.

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

El plan de trabajo puede ser elaborado con cualquier metodología existente de gestión de proyectos y debe reflejar los recursos disponibles, humanos, económicos, de conocimiento y de tiempo con los que se cuenta, considerando todo el ciclo de vida de los datos.

En ese sentido, un plan de trabajo debe contener al menos:

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

Caso Práctico

Plan de trabajo de la Institución "X"

La Institución "X" realiza un listado de todas las medidas de seguridad faltantes de acuerdo con su análisis de brecha. Considerando sus medios y sitios de resguardo, decide atender primero todas las medidas de seguridad que involucran el entorno de trabajo digital.

Código	Pregunta o control
A	**Medidas de seguridad basadas en la cultura del personal**
A.1.1	Política de escritorio limpio
A.1.3	Impresoras, escáneres, copiadoras y buzones limpios
A.1.4	Gestión de bitácoras, usuarios y acceso
A.2.2	Destrucción segura de la información en equipo de cómputo y medios de almacenamiento digital
A.2.3	Fijar periodos de retención y destrucción de la información
A.3.1	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos
A.3.2	Fomentar la cultura de la seguridad de la información
A.3.3	Difundir noticias en temas de seguridad.
A.3.4	Prevenir al personal sobre la Ingeniería Social
A.3.5	Asegurar la protección de datos personales en subcontrataciones
A.4.1	Tener un procedimiento de actuación y notificación
A.4.2	Realizar revisiones y auditorias
A.5.1	Respaldo en soportes documentales digitales
A.5.2	Periodicidad de respaldos
A.5.3	Resguardo de respaldo fuera de las instalaciones
B	**Medidas de seguridad en el entorno de trabajo físico**
B.2.3	Minimizar el riesgo oportunista
C	**Medidas de seguridad en el entorno de trabajo digital**
C.1.2	Actualización del software
C.3.2	Uso de contraseñas robustas
C.4.1	Hardening o endurecimiento de los equipos
C.4.2	Desactivación de la configuración por default
C.5.2	Reglas de navegación segura
C.5.3	Reglas para la divulgación de información
C.5.4	Uso de conexiones seguras
C.6.2	Envío seguro de la información

La Institución "X" se ha comprometido a cumplir ocho medidas de seguridad (marcadas en verde), en un plazo de seis meses, para ello ha solicitado se contemple la contratación de un especialista en seguridad. Asimismo, se contemplan pláticas de capacitación y sensibilización con los empleados, con la finalidad de que el equipo de trabajo conozca las medidas de seguridad que se están poniendo en marcha.

La decisión de la Institución "X" sobre qué controles implementar primero no fue a la ligera, entiende que implementar medidas de seguridad es un proceso que requiere dedicación. El entendimiento de su ciclo de tratamiento de datos personales lo ha hecho consiente de que la cantidad de información en sus equipos de cómputo lo obligan a atenderlos prioritariamente sobre otras consideraciones.

Una vez concluido el periodo de seis meses la Institución "X" evaluará sus avances y se planteará nuevos controles hasta cumplir con su lista de pendientes.

Resumen de la Etapa 3

¿Qué ha hecho la Institución "X" hasta este momento?

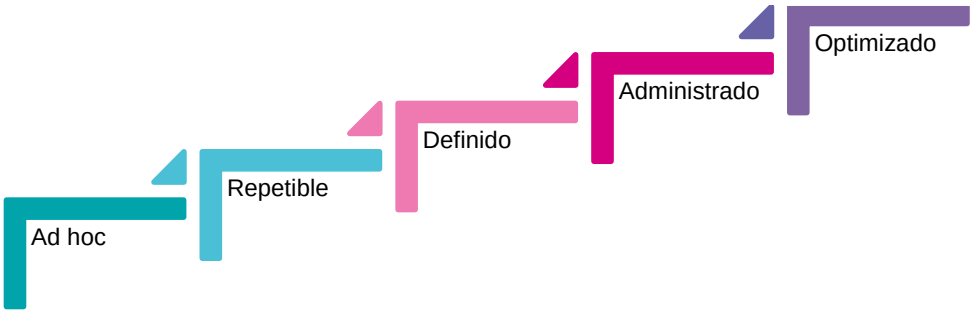
En esta etapa, la Institución logró:

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

2.4 Etapa 4. Mejora Continua

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

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



- **Ad Hoc:** Cada control de la Etapa 2 muy posiblemente empiece aquí, se pasó de no tener nada a tener una implementación dinámica, reactiva y con poca documentación.
- **Repetible:** Existe reglas claras sobre el control de seguridad, se pueden identificar resultados, aunque la disciplina todavía es poca.
- **Definido:** El control tiene un conjunto de reglas definidas y bien documentadas tanto en proceso como en personal involucrado.
- **Administrado:** El control posee indicadores y mecanismos que permiten monitorearlo y realizar actualizaciones afectando de manera mínima los procesos del Instituto.
- **Optimizado:** El control se enfoca en mejorar su despeño a través de mejores prácticas y las innovaciones tecnológicas que van surgiendo.

Existen circunstancias especiales en las que se tendrían que evaluar las posibilidades de aumentar el nivel y madurez en uno o más controles:

- Cuando haya crecimiento o un nuevo esquema de trabajo.
- Como resultado de la revisión o auditoría de un tercero.
- Debido a la ocurrencia de una vulneración a la seguridad de la información.

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

Importante

Sistema de Gestión en materia de protección de datos personales

El artículo 34 de la Ley de Datos, indica que, en un sistema de gestión, se deberán documentar las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales.

Un sistema de gestión para la protección de datos personales es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales. Algunas de las ventajas son:

- Permite rendir cuentas a los titulares y al órgano garante sobre el tratamiento de los datos personales en posesión del Instituto.
- Provee una estructura de los elementos que conforman la protección de datos personales.
- Ofrece una mejora continua a través de un enfoque sistémico.
- Facilita la verificación de que las medidas implementadas sean eficaces, eficientes y apropiadas de acuerdo con el riesgo inherente del dato personal.

En particular, el Sistema de Gestión para la Protección de Datos Personales, del Instituto, se encuentra integrado por las buenas prácticas nacionales e internacionales en protección de datos, privacidad y seguridad de la información, considera la mejora continua, es escalable, con relación a su alcance, para que las medidas sean coherentes con los riesgos personales y la naturaleza del dato personal, es compatible con otros sistemas de gestión y adaptable a diversos organismos públicos.

El Sistema de Gestión para la Protección de los Datos Personales, proveerá las bases para cumplir con los principios, deberes, derechos y demás obligaciones que señala la normatividad aplicable para permitir:

- Verificar que las medidas implementadas son eficaces, eficientes y apropiadas de acuerdo con el riesgo inherente del dato personal.
- Demostrar la conformidad de las actividades de tratamiento,
- Medir el aprovechamiento eficaz y permanente de los recursos destinados para el logro de los objetivos de protección de datos personales
- Integrar a toda la organización en la protección de los datos personales.

En este sentido, se determinaron 75 obligaciones o controles, agrupadas en 13 dominios que corresponden a los procesos de protección de datos personales. Cada dominio tiene un objetivo general y los controles cuentan con sus objetivos específicos. Los cuales tienen como finalidad describir lo que se debe lograr como resultado. A continuación, se enlistan los dominios:

1. **Política organizacional de protección de datos personales:** Para verificar que el Instituto disponga de pautas y criterios generales para la protección de los datos personales.
2. **Aspectos organizacionales de la protección de datos personales:** Para identificar a nivel institucional, los límites y alcances de las responsabilidades de los involucrados en la protección de los datos personales.
3. **Gestión de datos personales y mecanismos de transferencia y remisiones:** Con el fin de conocer los datos personales tratados, así como los procesos, propietarios, usuarios, custodios, encargados o terceros que intervienen durante su ciclo de vida, para verificar el cumplimiento con los principios de la protección de datos.
4. **Protección de datos personales en la operación:** Para asegurar que el tratamiento de los datos personales contempla las acciones necesarias para su protección.
5. **Protección de datos personales de los recursos humanos:** Para determinar las acciones mínimas para que los datos personales recabados, relacionados con el personal y prestadores de servicios del Instituto, sean debidamente tratados y asegurados.
6. **Gestión de la seguridad en el tratamiento de los datos personales:** Para llevar un control de las medidas de seguridad físicas, técnicas y administrativas mínimas para la protección de los datos personales.
7. **Riesgos con encargados:** Para verificar que los encargados protejan los datos personales bajo su resguardo.
8. **Avisos de Privacidad:** Con el fin de verificar que el Instituto dispone de avisos de privacidad con los requisitos que marca la Ley para dar cumplimiento al principio de información.
9. **Solicitudes ARCO:** Para verificar que el Instituto dispone de procedimientos que provean eficiencia al proceso de atención a solicitudes ARCO.
10. **Evaluaciones de impacto en la protección de datos personales:** Para verificar que se cuenta con una estrategia para los riesgos a los que están expuestos los datos personales-
11. **Gestión de vulneraciones:** Para verificar la existencia, vigencia y uso de procedimientos que permitan actuar de manera oportuna en caso de presentarse alguna vulneración de la seguridad de los datos personales.
12. **Monitoreo de la protección de los datos personales:** Para verificar la adecuada gestión en la protección de los datos personales con base en lo establecido en el sistema de gestión.
13. **Cumplimiento normativo:** Para verificar y generar evidencia del cumplimiento de la normatividad en la materia con base en el principio de responsabilidad.

Caso practico

La mejora continua de las medidas de seguridad de la Institución “X”

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

Para progresar en el nivel de sus controles a un nivel Repetible, la Institución “X” se dedicará a que las reglas y procedimientos que se han establecido se conviertan en reglas muy claras y se empiece a tener disciplina en el cumplimiento de ellas.

Cuando el personal de la Institución “X” atiendan de manera automática las reglas y procesos, el control habrá llegado a un nivel Definido, de forma tal que, si la Institución crece, a los nuevos integrantes podrán unirlos rápidamente a la cultura de la seguridad del consultorio.

Conforme el crecimiento y su conocimiento lo permita, la Institución “X” invertirá en tecnología para alcanzar los niveles de Administrado y Optimizado.

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

Resumen de la Etapa 4

¿Qué ha hecho la Institución “X” hasta este momento?

En esta etapa, la Institución logró:

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

3 MAPA DE LAS ACCIONES PARA LA SEGURIDAD

A continuación, se muestra un diagrama con las acciones que contempla el Manual para la Implementación de medidas de seguridad.

Etapa 1: Identificación del flujo de los datos personales			
Pregunta1: ¿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 y manejar los datos personales?**

Etapa 2: Evaluación de las medidas de seguridad (mediante análisis de riesgos y brecha)		
A. Medidas de seguridad físicas	**B. Medidas de seguridad técnicas**	**C. Medidas de seguridad administrativas**

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

Etapa 4. Mejora continua	
Implementación de todas las medidas de seguridad basicas	**Modelo de madurez**

4 ANEXOS

4.1 ANEXO A. INVENTARIO DE DATOS PERSONALES.

4.1.1 A.1. Tabla de identificación de tipos de datos personales

Datos personales recabados	¿Es necesario?	¿Por qué?
Datos de identificación y contacto		
Nombre		
Estado Civil		
Registro Federal de Contribuyentes (RFC)		
Clave Única de Registro de Población (CURP)		
Lugar de nacimiento		
Fecha de nacimiento		
Sexo/género		
Nacionalidad		
Domicilio		
Teléfono particular		
Teléfono celular		
Correo electrónico		
Nombre de usuarios en redes sociales		
Firma autógrafa		
Firma electrónica		
Edad		
Fotografía		
Referencias personales		

Datos personales recabados	¿Es necesario?	¿Por qué?
Datos sobre características físicas		
Color de piel		
Color de iris		
Color de cabello		
Señas particulares		
Estatura		
Peso		
Cicatrices		
Tipo de sangre		
Datos biométricos		
Imágenes del Iris		
Huella dactilar		
Fotografía		
Palma de la mano		
Datos laborales		
Puesto o cargo que desempeña		
Domicilio de trabajo		
Correo electrónico institucional		
Teléfono institucional		
Referencias laborales		
Información generada durante los procedimientos de reclutamiento, selección y contratación		
Experiencia/Capacitación laboral		

Datos personales recabados	¿Es necesario?	¿Por qué?
Datos académicos		
Títulos		
Cédula profesional		
Certificados		
Diplomados		
Reconocimientos		
Datos migratorios		
Entrada al país		
Salida del país		
Tiempo de permanencia en el país		
Calidad migratoria		
Derechos de residencia		
Aseguramiento		
Repatriación		
Datos patrimoniales y/o financieros		
Bienes muebles		
Bienes inmuebles		
Información fiscal		
Ingresos		
Egresos		
Cuentas bancarias		
Seguros		
Afores		

Datos personales recabados	¿Es necesario?	¿Por qué?
Datos sobre pasatiempos entretenimientos y diversión		
Pasatiempos		
Aficiones		
Datos sobre pasatiempos entretenimientos y diversión		
Deportes que practica		
Datos legales		
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)		
Otros datos personales		
Datos personales sensibles		
Datos sobre la ideología		
Posturas religiosas/ideológicas/ morales/ filosófica		
Pertenencia a un partido/Posturas políticas		
Pertenecía a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado o futuro		
Estado de salud mentar presente pasado o futuro		
Información genética		
Datos sobre la vida sexual		
Preferencias sexuales		
Practicas o hábitos sexuales		
Datos de origen étnico o racial		
Pertenencia a un pueblo, etnia o región		
Otros datos personales sensibles		

4.1.2 A.2. Tabla de identificación de soportes documentales de almacenamiento de datos personales y esquema de privilegios.

Soporte documental y formato de almacenamiento	Físico	Digital	¿Quiénes tienen privilegios de uso?
Correspondencia/Correo			
Formularios			
Copias de documentos de identificación			
Solicitudes			
Bases de datos			
Hojas de calculo			
Contratos			
Expedientes			
Audio y/o video			
Otros			

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

Sitio de resguardo	¿Qué medios de almacenamiento se resguardan?	¿Quiénes tienen privilegio de acceso?
Oficinas de la empresa		
Instalaciones de tercero		
Otros		
Medio de almacenamiento físico	**¿Qué soporte documental o medios de almacenamiento se resguardan?**	**¿Quiénes tienen privilegio de acceso?**
Escritorio/Cajones		
Estantes/Archiveros		
Bóvedas/cajas fuertes/cuartos de seguridad		
Carpetas/Organizadores		
Otros		
Medio de almacenamiento digital	**¿Qué soporte documental o formato de almacenamiento digital se resguardan?**	**¿Quiénes tienen privilegio de acceso?**
Computadoras de escritorio		
Computadoras portátiles (Laptop)		
Servidores propios		
Teléfonos inteligentes y otros dispositivos móviles		
Memorias USB, discos duros extraíbles y otros medios de almacenamiento		
Almacenamiento en línea/computo en la nube		
Otros		

4.2 ANEXO B. CATEGORIZACIÓN DELOS DATOS PERSONALES Y VALOR DE RIESGO ASOCIADO

4.2.1 B.1. Categorización por tipo de dato personal

Según el INAI, los datos se categorizan en los siguientes niveles (INAI, 2015):

I. **Estándar**. Datos de **identificación y contacto, laborales y académicos**, como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.

II. **Sensible.** Contempla los siguientes datos:

a. **De Ubicación física** de la persona, como la dirección física, relativa al tránsito de las personas dentro y fuera del país y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más (dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.).
b. **De patrimonio**. Todos aquellos que permitan inferir el patrimonio de una persona, incluye entre otros, saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados, número de tarjeta bancaria de crédito y/o débito.
c. **De autenticación,** información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.
d. **Jurídicos,** como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
e. **Todos aquellos que afecten la esfera más íntima de su titular**, es decir, los que puedan dar **origen a discriminación** o conlleven un **riesgo grave a la integridad del titular**, como revelar aspectos del origen racial o étnico, estado de salud, pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales, entre otros, según el caso en concreto.

III. **Especial.** Son todos los datos que, debido a su naturaleza o bien debido a un cambio excepcional en el contexto de las operaciones usuales, pueden causar daño directo a los titulares, como información adicional de la tarjeta bancaria -número de tarjeta de crédito o débito más cualquier otro dato relacionado o contenido en la misma (fecha de vencimiento, código de seguridad, datos de la banda magnética, número de identificación personal PIN)-.

Nota. Lo anterior es sólo una guía ya que, como lo señala el INAI, es posible que ciertos datos personales que, en principio no se consideran sensibles, pueden llegar a serlo dependiendo del contexto en el que la información sea tratada.

4.2.2 B.2. Identificación del nivel de riesgo

Posteriormente, se identifica el riesgo inherente a los datos de acuerdo con su criticidad (INAI, 2015):

I. **Bajo**. Considera información general como datos de identificación y contacto o información académica o laboral.
II. **Medio**. Contempla los datos:
    a. De ubicación física,
    b. De patrimonio,
    c. De autenticación,
    d. Jurídicos.
III. **Alto**. Datos personales que puedan dar origen a discriminación o conlleven un riesgo grave a la integridad del titular.
IV. **Reforzado**. Son **todos los considerados *datos especiales***.

4.3 ANEXO C. ANÁLISIS DE BRECHA

El siguiente es un ejemplo básico para la elaboración de un análisis de brecha únicamente aplicable al caso práctico. Cabe mencionar que, para realizar el análisis de brecha, se deberá solicitar la metodología y la herramienta a la UTyPDP. Se sugiere el uso del estándar ISO 27002:2013 para la selección de los controles.

Análisis de brecha de la Institución (Medidas de seguridad existentes vs medidas de seguridad faltantes)				
Código	**Pregunta de control**	**¿Existe?**		**Justificación**
		Sí	**No**	
B. Medidas de seguridad basadas en la cultura del personal - Medidas Administrativas -				
A.1	¿Evitas dejar a la vista información personal y llevas registro de su manejo?			
A.1.1	Política de escritorio limpio			
A.1.2	Hábitos de cierre y resguardo			
A.1.3	Impresoras, escáneres, copiadoras y buzones limpios			
A.1.4	Gestión de bitácoras, usuarios y acceso			
A.2	¿Tienes mecanismos para eliminar de manera segura la información?			
A.2.1	Destrucción segura de documentos			
A.2.2	Destrucción segura de la información en equipo de cómputo y medios de almacenamiento digital			
A.2.3	Fijar periodos de retención y destrucción de información			
A.2.4	Tomar precauciones con los procesos de reutilización			
A.3	¿Has establecido y documentados los compromisos respecto a la protección de datos?			
A.3.1	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos			

A.3.2	Fomentar la cultura de la seguridad de la información			
A.3.3	Difundir noticias en temas de seguridad			
A.3.4	Prevenir al personal sobre la Ingeniería Social			
A.3.5	Asegurar la protección de datos personales en subcontrataciones			
A.4	¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos?			
A.4.1	Tener un procedimiento de actuación y notificación			
A.4.2	Realizar revisiones y auditorias			
A.5	¿Realizas respaldos periódicos de los datos personales?			
A.5.1	Respaldo en soportes documentales digitales			
A.5.2	Periodicidad de respaldos			
A.5.3	Resguardo de respaldo fuera de las instalaciones			
B. Medidas de seguridad en entorno de trabajo físico -Medidas de seguridad Físicas -				
B.1	¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?			
B.1.1	Alerta del entorno de trabajo			
B.1.2	Mantener bitácoras del personal con acceso al entorno de trabajo			
B.2	¿Tienes medidas de seguridad para evitar el robo?			
B.2.1	Cerraduras y candados			
B.2.2	Elementos disuasorios			
B.2.3	Minimizar el riesgo oportunista			
B.3	¿Proteges el movimiento de información en entornos de trabajo físicos?			
B.3.1	Aprobación de salida de documentos equipo de cómputo y/o medios de almacenamiento electrónico			

B.3.2	Mantener en movimiento solo copias de la información, no el elemento original			
B.3.3	Usar mensajería certificada			
C. Medidas de seguridad en el entorno de trabajo digital - Medidas de seguridad Técnicas -				
C.1	¿Realizas actualizaciones del equipo de cómputo?			
C.1.1	Actualización del sistema operativo			
C.1.2	Actualización del software			
C.1.3	Actualización del hardware			
C.2	¿Revisas periódicamente el software instalado en el equipo de cómputo?			
C.2.1	Uso de software actualizado			
C.2.2	Restricción de uso de software distinto al Institucional para descargar o compartir archivos			
C.2.3	Verificación de licencias			
C.3	¿Tienes medidas de seguridad para acceder al entorno de trabajo digital?			
C.3.1	Uso de contraseña y/o cifrado			
C.3.2	Uso de contraseñas robustas			
C.3.3	Bloqueo y cierre de sesiones			
C.3.4	Gestión de usuarios y accesos			
C.4	¿Revisas la configuración de seguridad del equipo de cómputo?			
C.4.1	Hardening o endurecimiento de los equipos			
C.4.2	Desactivación de la configuración por default			
C.5	¿Tienes medidas de seguridad para navegar en entornos digitales?			
C.5.1	Instalar herramientas antimalware y de filtrado de trafico			
C.5.2	Reglas de navegación segura			

C.5.3	Reglas para la divulgación de información			
C.5.4	Uso de conexiones seguras			
C.6	¿Proteges el movimiento de la información en entornos de trabajo digitales?			
C.6.1	Validación del destinatario de una comunicación			
C.6.2	Envío seguro de información			

4.4 ANEXO D. EJEMPLOS DE VULNERACIONES A LA SEGURIDAD: CASOS PRÁCTICOS

A continuación, se presentan casos en los que existen vulneraciones y lo que se aprende en cada caso. Estos ejemplos pueden utilizarse para la capacitación y sensibilización de los empleados de las áreas de este Instituto.

Caso 1. Empleados que comparten datos

Un empleado de una institución recibe una oferta de trabajo, sin embargo, una de las condiciones de la propuesta laboral es que el empleado le proporcione a la institución que oferta el trabajo, la base de datos de los empleados de la institución de origen.

El empleado, con el objetivo de obtener el trabajo, proporciona la base de datos de la Institución de origen, la cual es utilizada para comenzar un reclutamiento extensivo, por lo que contactan a los trabajadores, mismos que hacen del conocimiento de la situación a los Directores de la Institución de origen.

Los trabajadores llevan el caso ante el INAI, ambas Instituciones reciben penalizaciones por el mal uso de los datos personales, la falta de capacitación de sus empleados, la falta de controles de seguridad y políticas y programas claros en busca de implementar la cultura de privacidad.

Aprendizaje

- Concientizar a los empleados sobre la ilegalidad de la acción.
- Restringir los privilegios a las bases de datos, es decir, que tengan acceso a las bases, solo las personas que son necesarias para realizar una actividad.
- Establecer e implementar un procedimiento disciplinario en caso de incumplimiento.
- Deben de mantener registros que permitan identificar a la persona que realizó una copia de la base de datos o exportó dicha base.

Caso 2. Transferencia de datos entre Instituciones

Una Institución pública decide compartir su base de datos con una Institución privada, con la finalidad de verificar información de ciudadanos, lo cual parece no tener ningún tipo de afectación, sin embargo, dicho intercambio de bases de datos lo realizan sin el consentimiento de los titulares de los datos personales, sin un instrumento jurídico donde se formalice la transferencia y para fines distintos para los que fueron recabados los datos.

Aprendizaje

- Las Instituciones deben de recabar el consentimiento de los ciudadanos para compartir sus datos.
- Los datos deben utilizarse exclusivamente para los fines para los que fueron recabados.

- La Institución debe de formalizar las transferencias mediante cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico.

Caso 3. Empleado que pierde documentación en un lugar público

Un empleado del área de atención ciudadana de la Institución atiende solicitudes relacionadas con los derechos ARCO, debido a las actividades de la oficina, no alcanza a concluir la atención de dichas solicitudes, por lo que decide llevarse trabajo, fuera del centro de trabajo establecido, con la finalidad de avanzar y dar respuesta a los solicitantes dentro del término establecido por la ley.

Dicho empleado, va a una cafetería a realizar su trabajo, el cual avanza, sin embargo, al organizar su documentación deja en una silla de la cafetería una cedula en la cual se encuentran los datos personales pertenecientes a una solicitud de derechos ARCO, entre ellos el nombre, domicilio, RFC, teléfono, etc., dicho documento lo encuentra un vendedor, mismo que ofrece sus servicios y visita al ciudadano en su domicilio. El ciudadano molesto solicita le informe cómo obtuvo sus datos, a lo cual el vendedor le entrega la cédula, misma que cuenta con el logotipo de la Institución, por lo que el titular de los datos presenta una denuncia ante el INAI.

El INAI realiza la investigación, indaga en la Institución y se da cuenta que no tiene medidas de seguridad para evitar fugas de información y que además no notificó al titular de los datos de dicha vulneración a la seguridad.

Aprendizaje

- Capacitar y concientizar a los empleados sobre las vulneraciones.
- Implementar procedimientos a ejecutar en caso de vulneraciones.
- Restringir los medios de almacenamiento físico y digital, y restringir la salida de información que contenga datos personales de las instalaciones de la Institución.