GUÍA DE MEJORES PRÁCTICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CON UN ENFOQUE PRÁCTICO

Sector Público

inai

DIRECTORIO

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

Av. Insurgentes Sur 3211,
Col. Insurgentes Cuicuilco,
Alcaldía Coyoacán,
C.P. 04530,
Ciudad de México.

ÍNDICE

INTRODUCCIÓN

Derivado de la obligación que tienen los sujetos obligados para dar cumplimiento a la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General)**, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto) pone a su disposición la presente guía que tiene como finalidad promover las mejores prácticas y generar una cultura de protección de datos personales desde un enfoque preventivo.

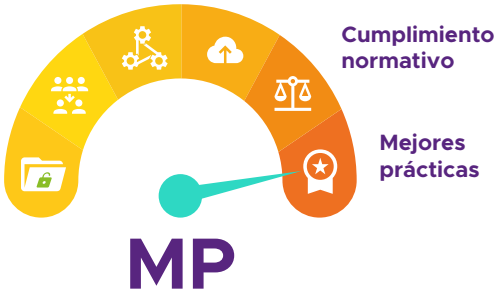
La guía comprende temas que hacen referencia a la importancia del uso de protocolos seguros para la navegación en internet o transferencia de información, encriptación, anonimización, así como, los beneficios de contar con un oficial de protección de datos personales, las ventajas de conocer el nivel de cumplimiento en materia de datos personales por medio de auditorías voluntarias y los beneficios de adoptar esquemas de mejores prácticas, entre otros.

Así mismo, se presenta un caso práctico, que permite armonizar la aplicación de la Ley General a través de la implementación del enfoque de privacidad desde el diseño, con la finalidad de que el sujeto obligado desarrolle criterios propios considerando el tipo de desarrollo o infraestructura que emplee para realizar el tratamiento de datos personales.

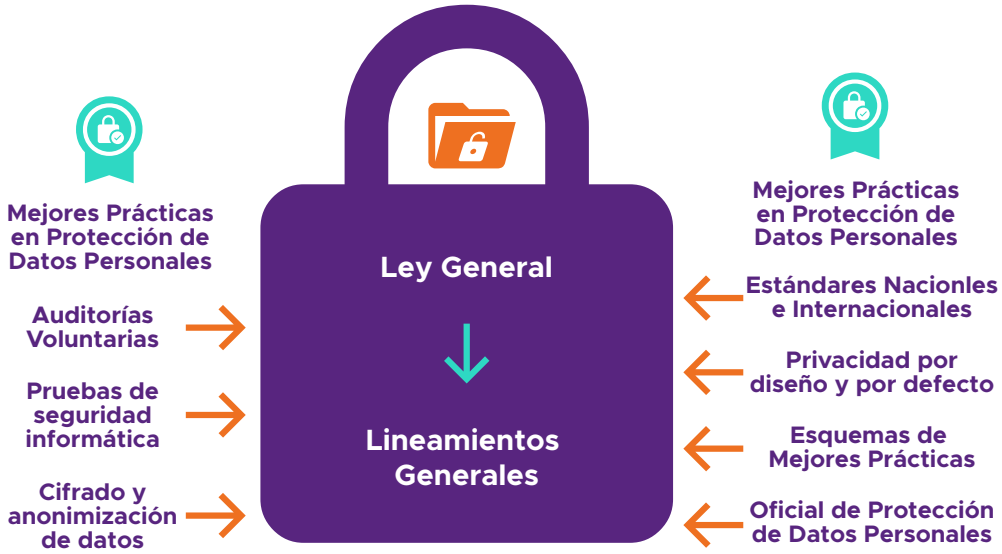
Es importante mencionar que, las mejores prácticas ayudan a elevar el nivel de protección de los datos personales, desarrollando o adoptando esquemas de mejores prácticas en la materia, de tal manera que puedan ser validados por el Instituto e inscritos en el Registro de Esquemas de Mejores Prácticas (REMP), lo que además, permite dotar de confianza a las personas titulares de los datos, quienes podrán consultar bajo que modalidad de Esquema de Mejores Prácticas el responsable o encargado del sector público, realiza el tratamiento de sus datos personales.

MEJORES PRÁCTICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Los responsables en sector público tienen la obligación de demostrar el cumplimiento en materia de protección de datos personales; sin embargo, ahora cuentan con la posibilidad de **elevar el nivel de cumplimiento establecido por la Ley General** realizando acciones preventivas en materia de protección de datos personales, con la aplicación de mejores prácticas[1].



Las **mejores prácticas en materia de protección de datos personales** pueden entenderse como medidas que, **los sujetos obligados** pueden adoptar y desarrollar de forma individual o grupal con otros responsables y encargados, con el objetivo de fortalecer la protección de los datos personales, además de promover, fomentar y difundir una cultura de su protección. A continuación, se mencionan algunos ejemplos de manera enunciativa más no limitativa de mejores prácticas en materia de protección de datos personales:



[1]Título Sexto de la Ley General.

VENTAJAS DE DESARROLLAR MEJORES PRÁCTICAS EN LA PROTECCIÓN DE DATOS PERSONALES:

- Fortalecer el cumplimiento de los principios, deberes y obligaciones establecidas en la Ley General.
- Resiliencia operativa con el tratamiento de los datos personales.
- Mayor capacidad para hacer frente a las amenazas constantes en la protección de datos personales.
- Posibilidad de inscripción en el REMP[2] y uso del distintivo REMP-INAI[3].
- Reducir los riesgos a los que se encuentran expuestos los datos personales.
- Mantener y proteger los activos del sujeto obligado bajo medidas de seguridad.
- Reforzar la implementación de controles y medidas de seguridad en el tratamiento de datos personales.
- Identificar mejoras en el diseño de sistemas.
- Contar con personal capacitado en la administración y operación de sistemas de tratamiento.
- Mejora continua en la protección de datos personales como parte de la cultura en el sujeto obligado.

Las mejores prácticas pueden realizarse o desarrollarse en el día a día, dentro de cada actividad sin darse cuenta, por ello, es necesario identificar que acciones han funcionado para ciertas actividades y documentarlas para medir su efectividad en el tratamiento.

[2]Consulta en: https://registro-esquemas.inai.org.mx/

[3]Consulta en: https://www.dof.gob.mx/nota_detalle.php?codigo=5479142&fecha=07/04/2017#gsc.tab=0

EJEMPLOS DE MEJORES PRÁCTICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

EJEMPLOS DE MEJORES PRÁCTICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Las mejores prácticas en materia de protección de datos personales se desarrollan fortaleciendo los procesos de tratamiento que tengan como finalidad elevar el nivel de protección de datos personales desde las diferentes áreas involucradas, así como, de los actores involucrados que participan en el diseño, desarrollo y puesta en marcha de los procesos de tratamiento. Lograr el trabajo en equipo es de vital importancia, ya que la protección de datos personales es un eje transversal en el que participan diversas áreas, por ejemplo, áreas legales, tecnologías de la información, personal que trata los datos, comité de transparencia, etc., por lo que, la coordinación será útil para poder desarrollar políticas que permitan llevar a cabo la implementación de controles que eleven el nivel de protección de los datos personales.

Los ejemplos que se mencionan a continuación permitirán a los responsables o encargados, identificar de manera general aquellos mecanismos que pueden adoptar como referencia para fortalecer los medios de comunicación, almacenamiento y en general de cada proceso de tratamiento, con la finalidad de mantener la confidencialidad, integridad y disponibilidad de los datos personales.

1. CIFRADO EN LA PROTECCIÓN DE DATOS PERSONALES

El cifrado o encriptación es un método de escritura que consiste en sustituir las palabras por otras, evitando la pérdida o exposición de información. De este modo, se sustituye la **información original** por otra que es **ilegible** a simple vista, por lo que, solo tendrá acceso a ella el personal con los medios para descifrarlo.

Ejemplo de comunicación cifrada

El cifrado está presente en diversas actividades cotidianas, desde navegar por internet, realizar pagos en línea, enviar mensajes de texto, entre otras, por lo que es una herramienta sumamente importante capaz de fortalecer la seguridad de información de millones de personas en todo el mundo. A continuación, se muestran algunos ejemplos cotidianos:

a) **Navegar en internet.** El Protocolo de Transferencia de Hipertexto Seguro **(https)**[4] permite establecer comunicaciones seguras a través de Internet, protegiendo la integridad de la comunicación entre un sitio web y los navegadores de un usuario, obteniendo mayor confianza y tranquilidad en los usuarios al navegar, comprar y trabajar.

[4] Protocolo de Transferencia de Hipertexto Seguro (en inglés, Hypertext Transfer Protocol Secure o HTTPS) le indica al navegador que encripte los datos intercambiados con una página web. La encriptación oculta los datos y reduce las posibilidades de que alguien vea o manipule su información, lo cual resulta importante cuando un sitio web incluye datos sensibles, como información personal o financiera.

b) **Mensajes de texto.** El cifrado de extremo a extremo *(del inglés end-to-end encryption o E2EE)* garantiza que la persona que envía y la que recibe puedan leer el mensaje original sin alteración o intervención durante la comunicación.

c) **Correo electrónico.** El cifrado en el envío y recepción de correos electrónicos disminuye el riesgo de que otras personas puedan espiar o interceptar la información mientras viaja, lo anterior, por la gran cantidad de tecnologías de transmisión, así como de proveedores de servicios de Internet.
Por ejemplo:

Outlook[5]

Google[6]

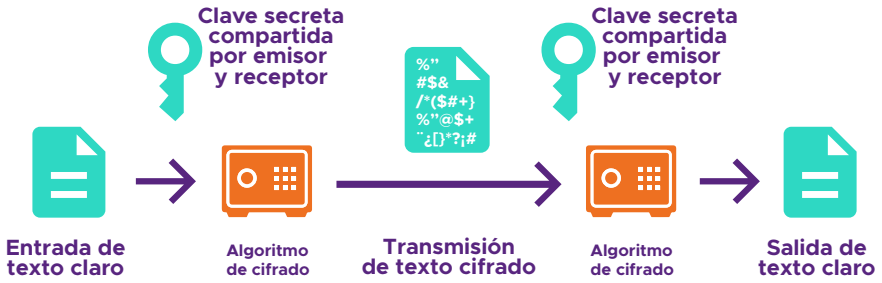
Tipos de cifrado

Los **principales tipos de cifrado** son el **cifrado simétrico** y el **cifrado asimétrico**, a continuación, se describe cada uno de forma general.

CIFRADO SIMÉTRICO

Es recomendable la utilización de cifrado simétrico en el tratamiento de los datos personales, ya que fortalece la seguridad para reducir el riesgo de que la información pueda ser extraída o reproducida por personas no autorizadas para hacerlo.

El cifrado **simétrico** es un término utilizado para los algoritmos criptográficos[7] que utilizan la misma clave para el **cifrado y el descifrado**. La clave se suele llamar "clave simétrica" o "clave secreta"[8]. La clave es aquella cadena de caracteres que debemos introducir tanto para cifrar como para descifrar el envío o recepción de información.



Criptografía simétrica

[5]Consulta en: https://support.microsoft.com/es-es/office/cifrar-mensajes-de-correo-373339cb-bf1a-4509-b296-802a39d801dc

[6]Consulta en: https://support.google.com/mail/answer/6330403?hl=es-419

[7]Un algoritmo criptográfico, es un algoritmo que puede encriptar texto en lenguaje natural para hacerlo legible, y para que sea de encriptado con el fin de recuperar el texto original. Consulta en: https://developer.mozilla.org/es/docs/Glossary/Cipher

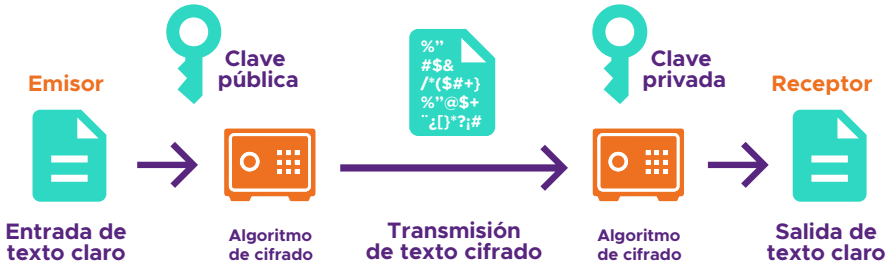
[8]Consulta en: https://developer.mozilla.org/es/docs/Glossary/Symmetric-key_cryptography

El cifrado permite traducir datos de texto sin formato (texto claro) en algo que parece ser aleatorio y sin significado (texto cifrado). Por su parte, el descifrado convierte el texto cifrado en texto sin formato. Para descifrar un fragmento determinado de texto cifrado, se debe usar la clave que se usó en un inicio para cifrar datos.

CIFRADO ASIMÉTRICO

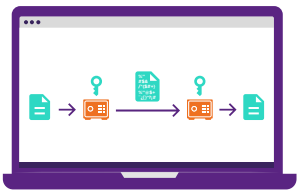
Este tipo de cifrado es una de las técnicas más potentes de la informática y parte fundamental de la seguridad de Internet. Su uso ha permitido altos niveles de seguridad, privacidad y anonimato.

La operación de este método utiliza una clave pública que permite enviar datos cifrados desde el emisor (el que envía - emisor) y la clave privada o secreta (el que recibe - receptor), que será el único que podrá descifrar los datos que envía el emisor.



Cifrado asimétrico

Con el objeto de familiarizarse con el uso del cifrado existen algunas páginas que permiten realizar ejercicios con el fin de familiarizarse en el uso del cifrado y descifrado, son las siguientes:



- Cifrar y descifrar texto en línea
- Criptografía online

Sugerencia de guías de consulta sobre el cifrado:

- Cifrado de datos
- Qué es encriptación
- Cifrado de datos en microsoft
- Criptografía en android

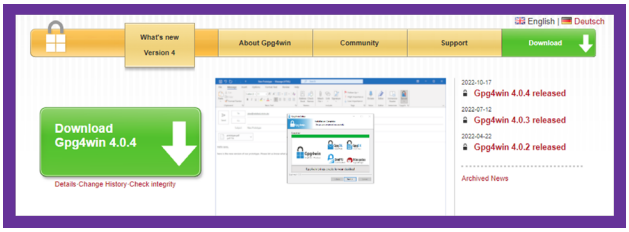
CASO PRÁCTICO DE CIFRADO ASIMÉTRICO

Existen herramientas que permiten fortalecer la seguridad de los archivos y mensajes que contienen datos personales que requieran la confidencialidad, disminuyendo la posibilidad de que puedan ser utilizados de formas no autorizadas.

En el cifrado asimétrico el usuario posee un par de llaves denominadas llave pública y llave privada. A continuación, se presenta un ejemplo para cifrar y descifrar una carpeta:

SOFTWARE REQUERIDO	ENLACE
GnuPG (GPG)	http://www.gpg4win.org

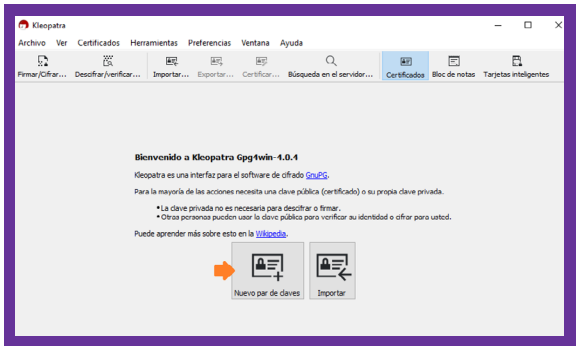
1.- Descargar e instalar Gpg4win



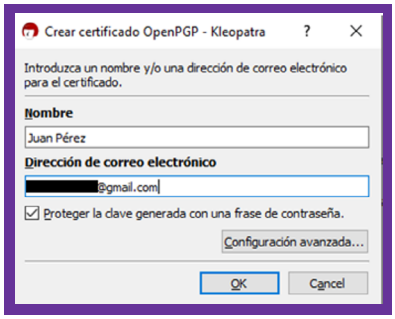
2.- Instalación de Kleopatra

3.- Generación de llaves

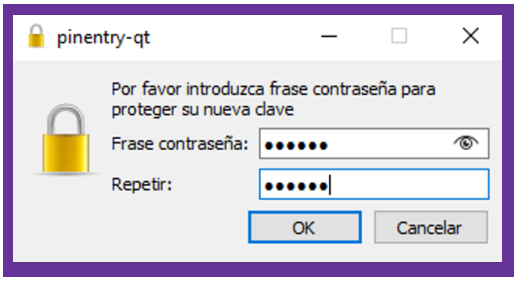
La **llave pública** puede utilizarse con distintas personas para cifrar información, sin embargo, solo podrán descifrar aquellas que tengan la llave privada.



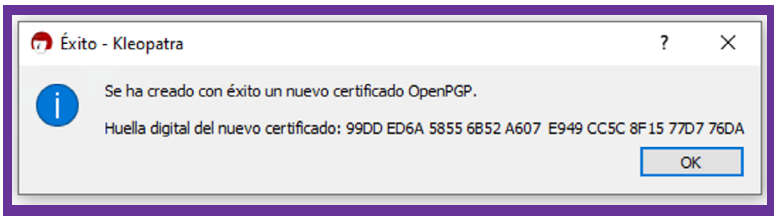
a) Llenar datos (nombre, dirección de correo electrónico), marcar la casilla Proteger la clave generada con una frase de contraseña.



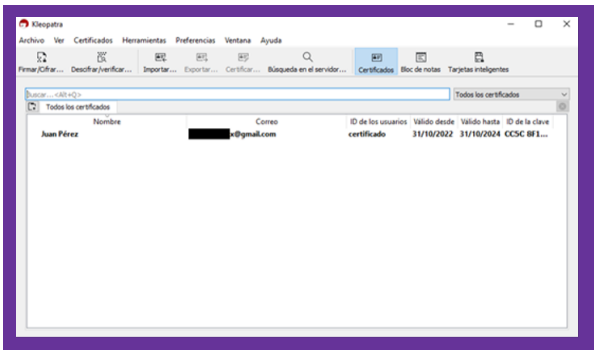
b) Asignar contraseña para uso de llave



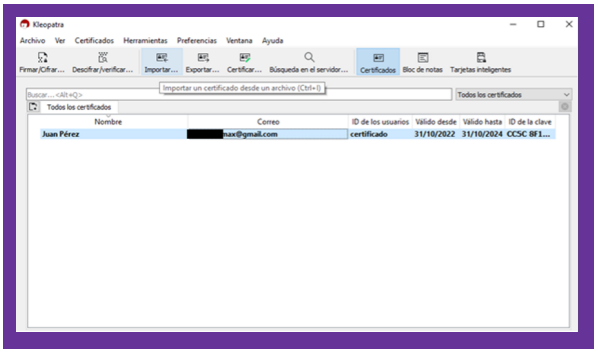
c) Se crea con éxito el certificado



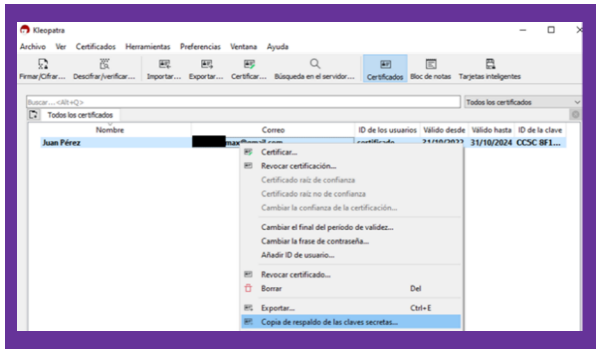
d) Pantalla que muestra la creación del certificado



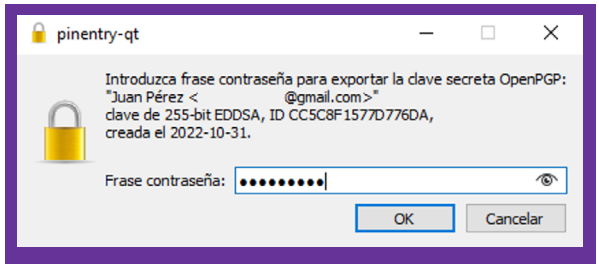
e) Exportar la llave pública y guardar



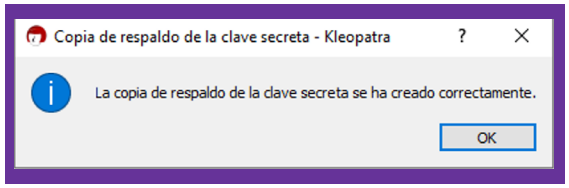
f) **Llave privada.** Se utiliza para descifrar, no es posible descifrar datos sin ella. Si requiere que más usuarios descifren un archivo, cada uno deberá generar un par de claves y compartir la pública con la persona que cifrará la información, pues es factible que el mismo archivo sea cifrado con diversas llaves públicas, de forma que cualquiera de ellos pueda extraer la información.



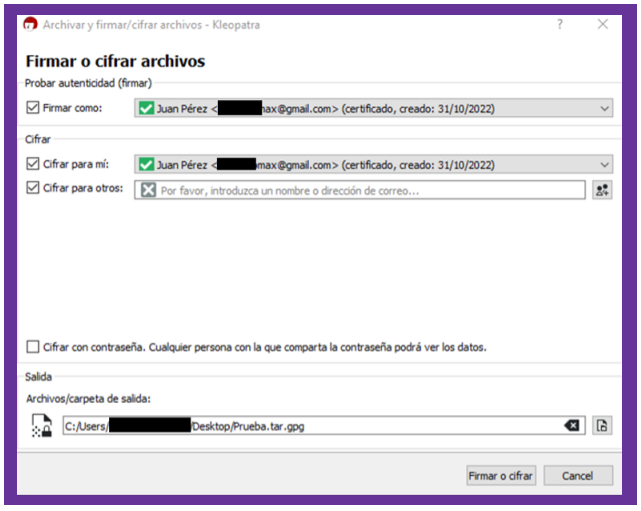
g) Asignar clave secreta para exportar la clave secreta.



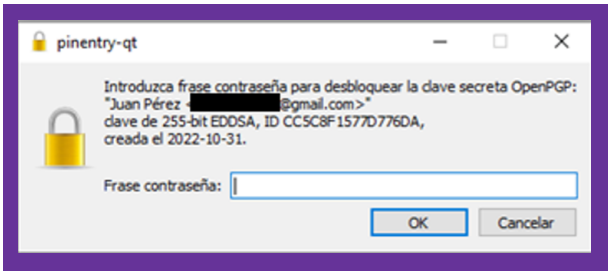
h) Guardar la clave secreta.



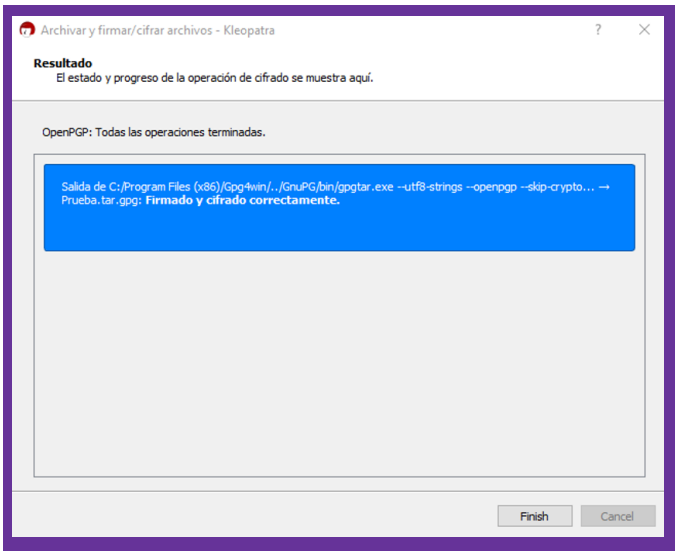
Para cifrar una carpeta o archivo, seleccione botón derecho (cifrar y firmar), posteriormente aparece el nombre del archivo o carpeta firmar y cifrar.



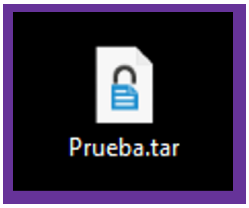
a) Introducir la firma pública que previamente se registro.



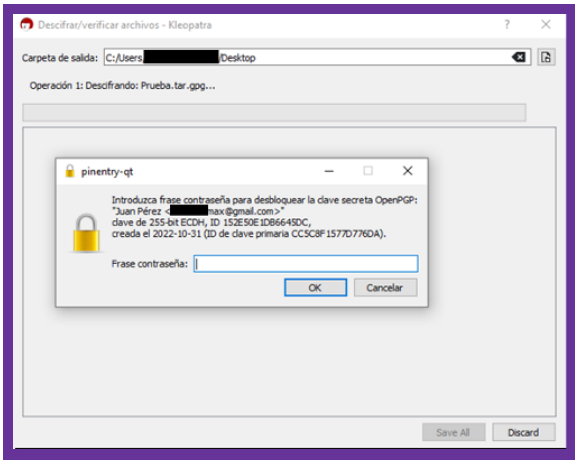
b) Mensaje que muestra que se ha cifrado el archivo.



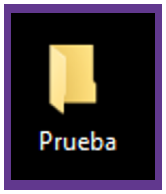
c) Se crea un archivo con extensión .tar.



5.- Proceso de descifrado. Con el botón derecho en el archivo o carpeta, seleccionar la opción descifrar y verificar (colocar la clave).



a) Se obtiene el archivo original



2. ANONIMIZACIÓN

La **anonimización de datos** se considera una mejor práctica que permite convertir los datos de tal forma que **no es posible identificar a los titulares de éstos**. Es una técnica que posibilita reducir los riesgos que se presentan en la obtención y tratamiento masivo de datos personales, es decir, la anonimización consistente en el proceso de identificar y ocultar información sensible, evitando su posible divulgación.

Un **ejemplo de anonimización** lo podemos ver implementado cuando se publican reportes o estadísticas de población escolar por comunidad, los datos (porcentajes) no se pueden usar para identificar a cada individuo que haya hecho la encuesta de escolaridad. En este tipo de encuestas suelen recopilarse datos personales como edad, escolaridad, sexo, dirección, nivel de estudios, situación socioeconómica, entre otros, y finalmente se ven representados de forma gráfica o estadística.

La **principal ventaja** de la anonimización es que, permite aislar los datos y mantiene la privacidad frente a intrusos, actuando como barrera contra riesgos externos.

Por lo anterior, es recomendable aplicar la anonimización en casos específicos donde exista un equilibrio entre seguridad y privacidad, de tal forma que los datos personales sigan siendo útiles.

Sugerencia de documentos sobre técnicas de anonimización:

- Anonimización de los datos Comisión Económica para América Latina y el Caribe (CEPAL).
- Guía de anonimización de datos estructurados, Archivo General de la Nación de Colombia
- Guía de anonimización - Uruguay
- Orientaciones y garantías en los procedimientos de anonimización de datos personales
- Lineamientos para la anonimización de datos del sistema nacional de estudios poblacionales para la salud
- Anonimización de datos y Cloud Discovery
- Malentendidos relacionados con la anonimización
- Cómo Google Anonimiza los datos

3. SEUDONIMIZACIÓN

La seudonimización, es la técnica de tratamiento de datos que preserva la privacidad ocultando los datos personales.

Un **ejemplo de seudonimización** es cuando sustituimos cualquier dato personal por un código o por un identificador numérico, es decir, el proceso de cambiar los datos personales por seudónimos.

Para realizar la técnica de seudonimización se pueden llevar a cabo las siguientes actividades de acuerdo con lo que establece la Comisión Económica para América Latina y el Caribe (CEPAL) [9]:

- Asignar un único seudónimo a cada objeto de la información personal identificable.
- El seudónimo debe ser utilizado en reemplazo de números de identificación formales, como cédula de identidad, licencias de conducir, cuenta bancaria, etc. Se recomienda que los seudónimos tengan la misma longitud y formato para aumentar la legibilidad.
- Tener en cuenta el impacto de los sistemas de información en la asignación de los seudónimos generados para uso interno, y no tener una relación entre uno y otro.
- Si se utilizan seudónimos para uso externo, estos deben ser diferentes a los seudónimos generados para su uso interno, y no tener una relación entre uno y otro.
- Establecer las técnicas criptográficas para llevar a cabo la incorporación de seudónimos que reemplacen las variables de identificación directa.

Diferencia entre anonimización y seudonimización[10]

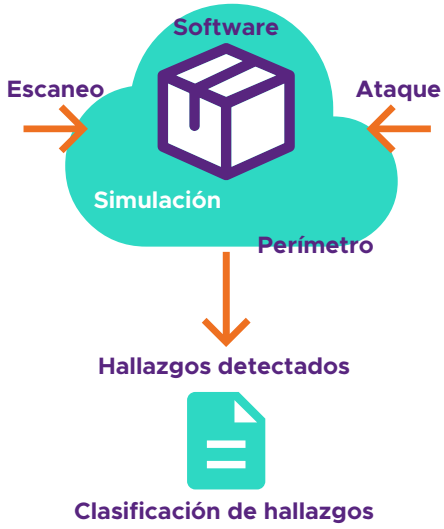
- La **anonimización** es un procedimiento donde los datos no sean posibles de identificar a los titulares de los datos personales.
- La **seudonimización** desvincula los datos identificativos, pero los datos seudonimizados mantienen datos adicionales que pueden reidentificar a los interesados, por tanto, es un procedimiento reversible.

4.PRUEBAS DE SEGURIDAD EN SOFTWARE

Las pruebas de seguridad en sistemas que contienen datos personales pueden ser sometidos a simulaciones de ataques reales para auditar posibles vulnerabilidades, brechas de seguridad, puntos débiles en un sistema de software y demostrar el impacto que esto puede ocasionar dentro de los tratamientos de datos personales.

[9]Consulta en: https://biblioguias.cepal.org/c.php?g=495473&p=4961125

[10]Consulta en: https://protecciondatos-lopd.com/empresas/seudonimizacion-anonimizacion/



Pruebas de seguridad (Penetration Testing).

El propósito de las pruebas de seguridad es identificar las debilidades potenciales para realizar una valoración con todas las variables que participan en la operación de los sistemas de tratamiento, como es el caso del personal en operación, la infraestructura, los activos, proveedores, herramientas de desarrollo, entre otros. Lo anterior permite prevenir la pérdida de información, accesos no autorizados, reputación de los responsables o encargados.

Las amenazas pueden provenir del exterior, por ejemplo, en casos de ataques informáticos, malware, robos de información, accesos no autorizados, etc. Así mismo, pueden ser procedentes del interior de la Institución conocido como amenazas internas, por ejemplo, errores humanos que borran la información por accidente, o generan una exposición pública de la información.

Se sugiere que las pruebas de seguridad se realicen durante todo el ciclo de vida de desarrollo de sistemas. Para esto, existen pruebas automatizadas, pero estas a veces omiten vulnerabilidades o marcan algunas que no lo son. Por lo que, se recomienda como una mejor práctica la implementación del **hacking ético**, en donde un equipo de expertos (que trabajen en la institución o trabajen de forma externa) que saben cómo piensan los cibercriminales, revisen los sistemas con la finalidad de encontrar vulnerabilidades que las herramientas automatizadas no consiguen.

Algunos beneficios de adoptar este tipo de prácticas son:

- Validar de forma integral los componentes de los sistemas de tratamiento.
- Identificar las vulnerabilidades en el proceso de desarrollo para actuar y remediar antes de la puesta en marcha de los sistemas de tratamiento.
- Alcanzar altas tasas de remediación cuando se implementan pruebas de seguridad continuas para localizar vulnerabilidades tempranas del desarrollo y remediarlas de forma casi inmediata.

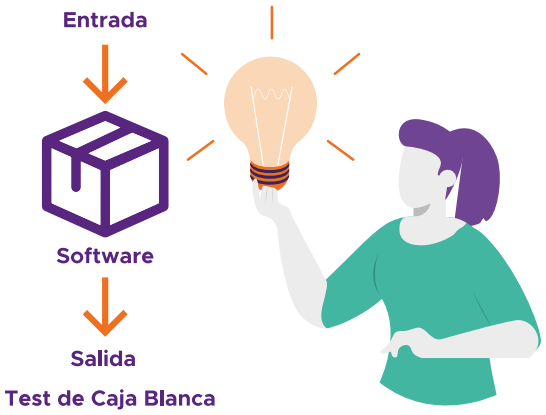
- Disminuir la posibilidad de cubrir costos altos al solucionar o arreglar de manera posterior los sistemas.
- Generar mayor confianza en la administración y operación de los sistemas de tratamiento.
- Mejorar la reputación del responsable en el cuidado de los datos personales.
- Obtener información e indicadores que permitirán mejorar los diseños de tratamiento de datos personales.
- Reducir los riesgos de pérdida o extracción de datos personales al interior o exterior de la Institución.
- Genera una cultura de monitoreo de vulnerabilidades a partir del conocimiento e información de fuentes abiertas de información, lo que permite diseñar simulacros de reacción ante los posibles impactos relacionados con los riesgos constantes en los sistemas de tratamiento.
- Contar con personal capacitado para prevención y reacción en caso de vulneración.

Existen dos alternativas para la implementación de las pruebas de seguridad:

1. **Expertos externos de pruebas de seguridad informática**, que permitan hacer pruebas de seguridad de software para detectar y solucionar los riesgos.
2. **Capacitar al personal de Tecnologías de la Información (TI)** de la Institución con el fin de desarrollar habilidades que les permitan revisar el diseño, desarrollo e implementación de los sistemas de tratamiento de datos personales previo a ser puestos en operación, lo anterior, permitirá establecer una cultura de monitoreo preventivo en las operaciones, con el fin de reducir el riesgo en el tratamiento de datos y poder establecer una mejora continua en los tratamientos.

Las pruebas de seguridad se pueden llevar a cabo de dos maneras, una de ellas es conociendo la infraestructura interna del responsable o encargado y la otra, sin conocer nada, a continuación, se describen cada una de ellas:

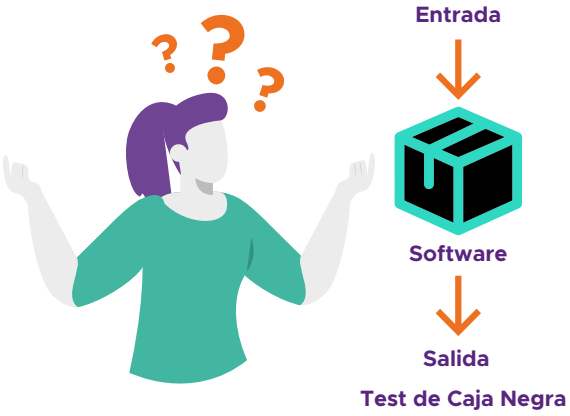
- **Pruebas de caja blanca** (White Box). Estas pruebas de seguridad informática interna permitirán auditar desde una perspectiva interna los ataques y vulneraciones posibles. Es más completo ya que parte de un conocimiento completo previo de la infraestructura a ser probada. Permitirá analizar que las pruebas a las que sean sometidos cumplan con los resultados esperados.



Mediante la prueba de la caja blanca el ingeniero del software puede obtener casos de prueba que[11]:

- Garanticen que se ejerciten por lo menos una vez todos los caminos independientes de cada módulo, programa o método.
- Ejerciten todas las decisiones lógicas en las vertientes verdadera y falsa.
- Ejecuten todos los bucles en sus límites operacionales.
- Ejerciten las estructuras internas de datos para asegurar su validez.

- **Pruebas de caja negra** (Black Box). Este tipo de pruebas se realizan sin tener conocimiento de la infraestructura que va a ser auditada, por lo que será sometida a distintos tipos de pruebas. Los tests de intrusión realizados deben ir precedidos de un acuerdo firmado donde se defina el alcance de este, así como las restricciones y/o limitaciones de las pruebas a los sistemas de tratamiento.



[11]Consulta en: https://www2.infor.uva.es/~jvalvarez/docencia/tema7.pdf

El método de la caja negra se centra en los requisitos fundamentales del software y permite obtener entradas que prueben todos los requisitos funcionales del programa. Con este tipo de pruebas se intenta encontrar[12]:

- ✓ Funciones incorrectas o ausentes.
- ✓ Errores de interfaz.
- ✓ Errores en estructuras de datos o en accesos a las bases de datos externas.
- ✓ Errores de rendimiento.
- ✓ Errores de inicialización y terminación.

Las áreas de pruebas de seguridad pueden realizarse de manera física, lógica y administrativa, algunos ejemplos de forma enunciativa más no limitativa son:

1. **Pruebas de seguridad en redes alámbricas e inalámbricas.** Permitirá poner a prueba la infraestructura bajo ataques que simulan diversos patrones aplicando las políticas de seguridad y controles de acceso desde diversos puntos de acceso.

2. **Pruebas de seguridad en aplicaciones web y móviles.** Las pruebas de seguridad de software permitirán resolver distintos tipos de vulnerabilidades que puedan existir en el diseño de su código, librerías e infraestructura de almacenamiento. Estas pruebas se clasifican en dos tipos:

    a) **Pruebas manuales.** En estas pruebas se usan scripts, donde se realiza manualmente el código sin ayuda de herramientas automatizadas, con el objetivo de comprender como funcionan las herramientas y se puedan descubrir las vulnerabilidades.

    b) **Pruebas automatizadas.** Es el uso de herramientas comerciales y de código abierto donde se realizan las pruebas bajo el escaneo de código de forma automatizada, comparando entre sus bases de datos aquellas vulnerabilidades que surgen día a día.

Sugerencias de herramientas y metodologías de pruebas de seguridad:

- Metodología de pentest.
- Kali Linux.
- Open Web Application Security Project (OWASP).
- Evaluador online de expresiones regulares en PHP,js y Python.
- OSINT Framework

[12]Consulta en: https://www2.infor.uva.es/~jvalvarez/docencia/tema7.pdf

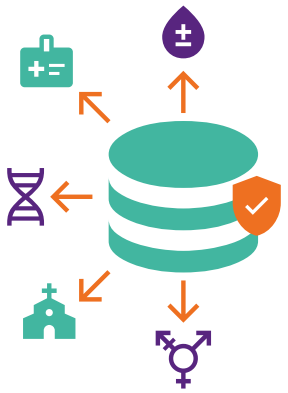
PRIVACIDAD DESDE EL DISEÑO

5. PRIVACIDAD DESDE EL DISEÑO

La privacidad desde el diseño (Privacy by Design, PbD)[13] es un término propuesto por Ann Cavoukian[14], Comisionada de Información y Privacidad de Ontario, Canadá, el cual tiene como objetivo integrar la privacidad en la propia arquitectura de la tecnología que se quiera desarrollar o implementar.

Es un tipo de metodología que permite establecer de manera proactiva y preventiva los principios, deberes y obligaciones que se establecen en la Ley General, en la planeación de los desarrollos tecnológicos que traten datos personales, así como la participación de todas las áreas involucradas y del personal especializado.

La siguiente imagen muestra la participación de equipos de trabajo legal y técnico para la construcción de una base de datos que cumpla con las medidas de seguridad adecuadas de acuerdo con los datos que van a tratarse y en cumplimiento con la Ley General.



Planeación de la construcción de una base de datos que tratará datos personales

La privacidad desde el diseño se soporta en 7 principios, que han sido adaptados al contexto del sector público, con el fin de poder brindar a los responsables y encargados una adaptación en sus tratamientos:

[13]Consulta en: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[14]Consulta en: https://gpsbydesigncentre.com/

1.- Proactivo, no Reactivo; Preventivo no Correctivo

Medidas proactivas para prevenir y anticipar riesgos e impactos a los derechos de los titulares antes de que ocurran. La planeación de los sistemas de tratamiento donde participen las áreas que intervienen en el proceso, atendiendo el cumplimiento normativo.

2.- La privacidad como configuración predeterminada

Cualquier tecnología o desarrollo tecnológico debe tomar en consideración desde la fase inicial de diseño los principios, deberes y obligaciones de protección de datos personales.

3.- La privacidad incrustada en el diseño

La privacidad debe convertirse en una parte esencial que fortalezca la seguridad y que por defecto mantenga las medidas de seguridad adecuadas desde el diseño. Definir las medidas de seguridad de manera preventiva, permitirá tener escenarios para la gestión de riesgos, recursos y personal, entre otros.

4.- Funcionalidad total – Todos Ganan

Lograr un equilibrio entre las áreas involucradas que permita dar el cumplimiento requerido, logrando acreditar mediciones que favorezcan el desempeño óptimo para todos. Así mismo al lograr marchar de manera conjunta, el resultado será lo óptimo para el titular de los datos personales.

5.- Protección durante el ciclo de vida

Es importante que los desarrollos de tratamiento se validen en cada inicio y termino de cada fase del ciclo de vida, con el fin de ajustar de ser necesario y lograr el cumplimiento propuesto desde la fase inicial.

6.- Transparencia, visibilidad y apertura

El desarrollo deberá realizarse con toda transparencia entre los involucrados de inicio a fin, con la finalidad de tener la certeza y participación en cada decisión, para este ejercicio se recomienda la elaboración por ejemplo de minutas, acuerdos, oficios o aquella documentación que permita seguir los acuerdos entre las partes.

7.- Enfoque centrado en el usuario

Es responsabilidad del responsable o encargado velar por la protección de los datos personales de los titulares, implementando todos los mecanismos que considere adecuados para fortalecer el tratamiento de datos personales en todas sus fases.

Sugerencia de material de consulta:

- Guía de Privacidad desde el Diseño

CASO PRÁCTICO

La aplicación de la **Privacidad desde el diseño** tiene una cualidad muy importante de adaptación de acuerdo con el sector, entorno y variables que pueden influir en su aplicación. Así mismo, podrá aplicarse con alcance normativo de manera total o parcial en cuanto a los principios, deberes u obligaciones de acuerdo con el artículo 11 y respecto al alcance material total o parcial de acuerdo con el artículo 12 de los Parámetros.

- **Como ejemplo**, se propone el diseño de una base de datos que almacenará datos personales de los titulares afiliados al sector salud con acceso a medicamentos controlados de la farmacia por lo que, se considera atender de manera parcial la normativa, por cuanto hace solo al deber de seguridad aplicando de manera general la privacidad desde el diseño.

- **Implementación**. En este punto, se tiene considerada la privacidad desde el diseño como una oportunidad, que de manera preventiva dará cumplimiento a la normativa de protección de datos personales de manera parcial.

En líneas generales, para el cumplimiento de la privacidad desde el diseño se deben integrar sus principios fundacionales en los procesos de diseño de productos y servicios. Los principios en cuestión son los siguientes:

1.- **Proactivo, no reactivo; preventivo, no correctivo**. En el diseño de la base de datos deberán identificar aquellos factores que permitan planear el diseño, desarrollo y puesta en marcha de ésta, integrando todas aquellas medidas de seguridad acorde al tipo de tratamiento al que este considerado. Deberán adherirse al diseño de la base aquellos elementos que fortalezcan la privacidad, por ejemplo, el desarrollo e implementación de políticas de protección de datos personales ya que son de inicio las que marcan el nivel de compromiso en la aplicación de las medidas de seguridad.

Cualquier sistema de tratamiento que utilice datos personales debe colocar la privacidad como una prioridad máxima desde el comienzo del proceso en diseño. Es importante, que el responsable coordine esfuerzos entre las áreas especialistas en el tratamiento de datos personales. Cabe señalar que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, es recomendable reunir al grupo de tecnología y el grupo legal, a fin de contar con una planeación que dé cumplimiento a la ley General.

2.- **La privacidad como configuración predeterminada**. Es obligación de los responsables o encargados mantener las medidas de seguridad adecuadas en los tratamientos de los datos personales con el fin de evitar su exposición. Para el ejemplo de la base de datos, se sugiere que ésta contenga controles administrativos, físicos y técnicos que permitan su operación óptima de acuerdo con los roles y responsabilidades de las personas servidoras públicas y/o encargados. Se recomienda que la base de datos cuente con mecanismos que permitan su administración, definida desde la fase anterior, tomando en consideración todos aquellos elementos que participen en su operación, ya sea de manera local o remota, el tipo de lenguaje de programación que se utilizará, el soporte técnico, las pólizas de contratación, copias de seguridad, cifrado, entre otras variables de acuerdo con el tipo de datos a los que se dará tratamiento, la cantidad de personas titulares y la finalidad del tratamiento.

3.- **La privacidad incrustada en el diseño**. Contempla todos aquellos elementos que fortalecen el tratamiento de los datos personales como es el caso de la base de datos, por ejemplo, las mejores prácticas en diseño y desarrollo de bases de datos, disociación de datos, cifrado, anonimización, pruebas de seguridad, respaldos y todos aquellos elemen-

tos que fortalezcan las medidas de seguridad y brinden mayor privacidad desde la parte administrativa, física y técnica.

4.- **Funcionalidad total – Todos Ganan.** Se sugiere que, en esta fase, se comprenda de manera integral el flujo de los datos personales de la base, desde su obtención hasta su eliminación, y que en cada proceso se puedan verificar los objetivos de cumplimiento con respecto a los criterios o controles de seguridad definidos en la primera fase, lo que brindaría mayor certeza en su funcionamiento obteniendo indicadores de cumplimiento.

5.- **Protección durante el ciclo de vida.** Durante el desarrollo de la base de datos, se recomienda realizar pruebas que vayan enfocadas en el cumplimiento normativo (atendiendo los principios, deberes y obligaciones), puede apoyarse en mejores prácticas y estándares nacionales o internacionales que permitan implementar medidas adecuadas para proteger la información, como por ejemplo la seudonimización, anonimización, cifrado y destrucción segura y garantizada de información al final del ciclo de vida.

En este ejemplo, solo se atiende el deber de seguridad, por lo que es importante ir validando en cada etapa de desarrollo de software con respecto a las políticas y controles de seguridad propuestos en la fase 1, con su alcance.

Es importante, validar cada fase con el personal encargado del cumplimiento en materia de protección de datos personales (oficial de datos personales, comité de transparencia, áreas involucradas en el tratamiento, áreas de tecnología y legales, etc.).

6.- **Transparencia, visibilidad y apertura.** Es recomendable que el proceso de desarrollo sea transparente desde los cimientos hasta su finalización, con reuniones periodicas del personal involucrado en la parte de cumplimiento (administrativo, legal, tecnológico, etc.) con el fin de ir validando los avances mediante minutas, correos, o cualquier documento que evidencie el conocimiento para todos los interesados en el desarrollo del proyecto, para nuestro caso de la base de datos.

7.- **Enfoque centrado en el usuario.** El responsable tiene el deber de cuidar y proteger los datos personales de las personas titulares, bajo las medidas de seguridad de acuerdo con sus recursos disponibles, infraestructura, personal, entre otros elementos, pero siempre con el compromiso de brindar confianza a las personas titulares en el tratamiento de sus datos personales.

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

6. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales **relevantes o intensivos**[15], **podrán** designar a un **oficial de protección de datos personales** que forme parte de la **Unidad de Transparencia**, lo cual, se considera una mejor práctica, debido a que permitirá fortalecer a la Institución de personal con conocimiento, cualidades profesionales y experiencia en materia de protección de datos personales.

Al respecto el considerando 23[16] de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, **reconoce la importancia de la adopción de medidas preventivas** que permitan a los responsables responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales, como lo es, la **designación de un oficial de protección de datos personales** que permite fortalecer el nivel de protección de los datos personales.

> “Es importante señalar que, para la designación del oficial de protección de datos personales, la Ley General no exige ningún perfil en específico para su nombramiento, sin embargo, se sugiere que se sigan las prácticas que en este tipo de actividades realiza el responsable de acuerdo con su sector”

Algunas **ventajas** de contar con un oficial de datos personales:

- Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.
- Participar con el Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.
- Proponer al Comité de Transparencia políticas, programas, acciones y otras actividades que permitan dar cumplimiento a la norma.
- Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales y las actividades que determine el responsable.

---

[15]Un tratamiento intensivo de datos personales se refiere a un tratamiento que por su magnitud o importancia implica un riesgo potecial. Es decir, cuando existan riesgos inherentes a los datos personales, datos personales sensibles o bien, se realicen o pretendan realizar transferencias de datos personales.

[16]Consulta en: https://www.redipd.org/es/documentos/estandares-iberoamericanos

A continuación, se muestra el fundamento normativo, así como una lista de Oficiales de Datos Personales. Los datos contenidos en el listado fueron encontrados en las páginas de los sujetos obligados de acceso público:

	LGPDPPSO	LINEAMIENTOS	OBLIGATORIO	MEJOR PRÁCTICA	ESTÁNDAR IBEROAMERICANO	ISO
OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	**ARTÍCULO 85**	**ARTÍCULOS 121 Y 122**	**NO**	**SI**	**23**	**27001**

Consulta lista de Oficiales de Datos Personales

De una encuesta realizada a **223** sujetos obligados federales, se reporta que solo el **17.48%** cuentan con Oficial de Protección de Datos Personales[17].

Guías de consulta nacional

Recomendaciones para los Sujetos obligados en la Designación del Oficial de Protección de Datos Personales.

Guías de internacional

Artículo 38[18]

Artículo 39[19]

Unión Europea.
Reglamento General de Protección de Datos Personales.

El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

Funciones del delegado de protección de datos
- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

- Delegado de Protección de Datos (DPD).

[17]Elaboración propia de la Dirección General de Prevención y Autorregulación del INAI

[18]Consulta en: https://www.privacy-regulation.eu/es/38.htm

[19]Consulta en: https://www.privacy-regulation.eu/es/39.htm

- Oficial de Datos Personales

- Decreto 620 de 2020. Oficial de Protección de Datos como figura obligatoria en Colombia

- Delegado de Protección de Datos Personales

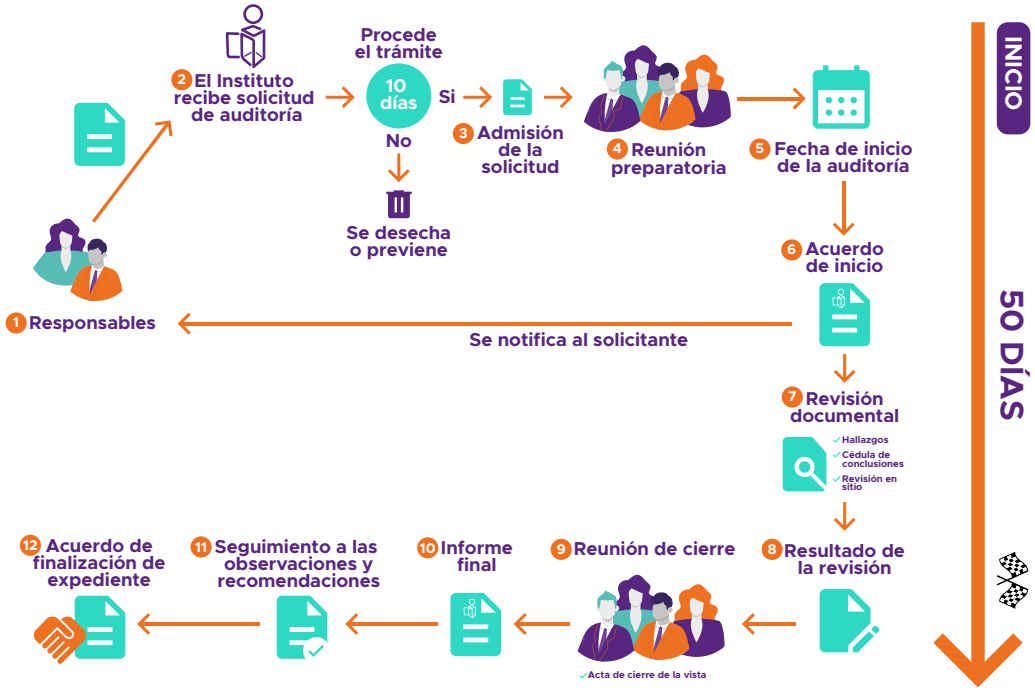
AUDITORÍAS VOLUNTARIAS

7. AUDITORÍAS VOLUNTARIAS EN PROTECCIÓN DE DATOS PERSONALES

El artículo 151 de la Ley General en concordancia con los artículos 1 y 218 de los Lineamientos Generales, establecen que los sujetos obligados del ámbito federal, pueden voluntariamente someterse a la realización de auditorías voluntarias por parte del Instituto, cuyo objeto es **verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la LGPDPPSO**, los Lineamientos Generales y demás normatividad que resulte aplicable.

Las auditorias voluntarias se consideran una mejor práctica, en virtud de que permite a los responsables y encargados conocer si los controles y mecanismos que tienen implementados son adecuados para el debido cumplimiento de la Ley General, sin ser vinculatoria y de manera gratuita.

A continuación, se muestra de manera general los pasos de la auditoría voluntaria:



1.- La auditoría siempre deberá iniciar a petición del sujeto obligado, el cual podrá presentar directamente su solicitud en el domicilio del Instituto, o bien, a través de cualquier otro medio habilitado para tal efecto (auditoriasvoluntarias@inai.org.mx).

2.- **El Instituto recibe la solicitud de auditoría voluntaria**. La cual deberá hacerse por escrito en el que se señalen los requisitos establecidos en el artículo 221 de los Lineamientos Generales:

- La denominación y el domicilio del responsable solicitante.
- Las personas autorizadas para oír y recibir notificaciones.
- La descripción del tratamiento de datos personales que se pretende someter a la auditoría voluntaria, indicando, de manera enunciativa más no limitativa:

- Las finalidades de éste;
- El tipo de datos personales tratados;
- Las categorías de titulares involucrados;
- Las transferencias que, en su caso, se realicen;
- Las medidas de seguridad implementadas;
- La tecnología utilizada, así como cualquier otra información relevante del tratamiento a auditar.

- Las circunstancias o razones que lo motivan a someterse a una auditoría voluntaria.
- El nombre, cargo y firma de quien solicite la auditoría voluntaria, que podrá ser el titular de la dependencia o entidad u homólogo, el titular de la unidad administrativa u homólogo que será auditada, el Oficial de Protección de Datos Personales del responsable o el Presidente del Comité de Transparencia.
- Cualquier otra información o documentación que considere relevante hacer del conocimiento del Instituto.

3.- **Admisión de la solicitud:** De conformidad con el artículo 222 de los Lineamientos Generales, una vez que el Instituto reciba la solicitud de auditoría voluntaria, contará con un plazo máximo de diez días hábiles, contados a partir del día siguiente de la recepción de la solicitud, para que la Secretaría de Protección de Datos Personales emita el acuerdo de admisión de la solicitud de auditoría voluntaria, o bien, para que la Dirección General de Prevención y Autorregulación (DGPAR), realice un requerimiento de información al responsable, en caso de que la solicitud no sea clara, o cuando se omita alguno de los requisitos de procedencia.

4.- **Reunión preparatoria**. Una vez que se haya admitido la solicitud de auditoría, la DGPAR deberá llevar a cabo una reunión de trabajo con el responsable solicitante, en la fecha acordada con éste.

La reunión de trabajo tiene, entre otros, los siguientes objetivos:

- Que el equipo auditor conozca los antecedentes y generalidades del tratamiento o procesos y de los controles, medidas o mecanismos implementados en materia de protección de datos personales que se revisarán en la auditoría;
- Establecer los objetivos y actividades generales de la auditoría, y
- Determinar con precisión el alcance de la auditoría.

Al finalizar la reunión de trabajo, se deberá levantar el acta circunstanciada correspondiente, en la que se incluirá, al menos, el alcance de la auditoría y, en su caso, la información o documentación que sea requerida por la DGPAR para continuar con el procedimiento.

5.- **Fecha de inicio de la Auditoría**. Una vez analizada la información y documentación aportada por el responsable solicitante en la reunión de trabajo y, en su caso, en el desahogo de los requerimientos de información de la DGPAR, esta última propondrá al responsable solicitante una fecha para **iniciar la auditoría**.

Para proponer la fecha de inicio de las auditorías voluntarias, la DGPAR podrá priorizar su atención a partir de la importancia, utilidad social, contexto y naturaleza de los procesos o tratamientos que se soliciten auditar.

La fecha de inicio de la auditoría se acordará entre las partes.

6.- **Acuerdo de Inicio de la Auditoría**. La DGPAR emitirá un acuerdo de inicio, el cual deberá contener, entre otros, los siguientes elementos:

- Fecha de inicio de la auditoría voluntaria;
- Servidor público que fungirá como auditor líder, quien será el encargado de la coordinación de la auditoría;
- Los objetivos de la auditoría voluntaria;
- El alcance de la auditoría voluntaria, incluyendo la identificación de las áreas a auditar; el tratamiento de datos personales; las finalidades del tratamiento; el tipo de datos personales tratados; las categorías de titulares involucrados; las transferencias que, en su caso, se realicen; las medidas de seguridad implementadas; la tecnología utilizada, entre otros elementos;
- Los criterios de auditoría;
- El servidor público facultado para representar al responsable solicitante en la auditoría voluntaria;
- Los asuntos relacionados con la confidencialidad y la seguridad de la información;
- Requerimientos de información y documentación relacionada con el tratamiento de datos personales que se someterá a la auditoría voluntaria, adicional a la que se haya aportado en la solicitud y en la reunión de trabajo, que resulte necesaria para continuar con el desarrollo de la auditoría.

7.- **Revisión documental**. El equipo auditor podrá determinar si las políticas, programas, procedimientos, prácticas o cualquier otra acción documentada están conforme con lo dispuesto por la Ley General, los Lineamientos Generales y demás normatividad aplicable.

8.- **Resultados de la revisión documental**.
La DGPAR podrá determinar los resultados de la revisión documental:

a) La conclusión de la auditoría, para lo que se emitirá el informe final correspondiente

b) La orden de visita de auditoría, que dará continuidad a las actividades de revisión en las instalaciones señaladas por el responsable y bajo los términos asentados en el acuerdo de inicio.

En el caso del inciso a, las partes acordarán fecha para la reunión de cierre para presentar los hallazgos y las conclusiones de la auditoría voluntaria, previo a la emisión del informe final.

En todo caso, las conclusiones de la revisión documental deberán quedar por escrito en las cédulas correspondientes y deberán considerarse para el informe final.

9.- **Reunión de cierre**. Las partes acordarán la fecha para la reunión de cierre para presentar hallazgos y las conclusiones de la auditoria, previo a la emisión del informe final.

10.- **Informe Final**. Es el documento en el cual se señalan los resultados obtenidos de la auditoria bajo los señalamientos de conformidades y no conformidades, lo que permitirá orientar al responsable sobre el fortalecimiento y un mejor cumplimiento de las obligaciones previstas en la Ley General y Lineamientos Generales. El Instituto deberá notificar al responsable auditado el informe final a que se refiere el presente artículo dentro de los cinco días siguientes contados a partir de la emisión del informe.

11.- **Seguimiento a las observaciones**. El instituto podrá pedir al responsable auditado que informe sobre la implementación de las recomendaciones que hayan sido emitidas en el informe final de la auditoría conforme a los términos y plazos establecidos el mismo informe.

El responsable auditado deberá responder el requerimiento del Instituto en un plazo máximo de diez días hábiles, contados a partir del día siguiente a la recepción del requerimiento.

12.- **Acuerdo de finalización de expediente**. Una vez concluida la totalidad de actividades de la auditoría voluntaria, la Secretaría de Protección de Datos Personales deberá instruir a la DGPAR para que elabore el acuerdo de cierre correspondiente, el cual será suscrito por la primera.

Normatividad aplicable a las Auditorias voluntarias

NORMATIVA	ARTÍCULOS
Ley General	151
Lineamientos Generales	1 y del 218 al 231
Manual de Procedimientos para la Realización de Auditorías Voluntarias	

Requisitos de la solicitud de auditaría voluntaria:

La solicitud para que se realice una auditoría voluntaria por parte del Instituto, deberá hacerse por escrito, en el que se señalen los requisitos establecidos en el artículo 221 de los Lineamientos Generales, los cuales son los siguientes:

- La denominación y el domicilio del responsable solicitante;
- Las personas autorizadas para oír y recibir notificaciones;
- La descripción del tratamiento de datos personales que se pretende someter a la auditoría voluntaria, indicando, de manera enunciativa más no limitativa;
  - las finalidades de éste;
  - el tipo de datos personales tratados;

- las categorías de titulares involucrados;
- las transferencias que, en su caso, se realicen;
- las medidas de seguridad implementadas;
- la tecnología utilizada, así como cualquier otra información relevante del tratamiento a auditar;

- Las circunstancias o razones que lo motivan a someterse a una auditoría voluntaria;
- El nombre, cargo y firma de quien solicite la auditoría voluntaria, que podrá ser el titular de la dependencia o entidad u homólogo, el titular de la unidad administrativa u homólogo que será auditada. el Oficial de Protección de Datos Personales del responsable o el Presidente del Comité de Transparencia; y
- Cualquier otra información o documentación que considere relevante hacer del conocimiento del Instituto.

Es importante señalar que, el responsable solicitante deberá especificar denominación y domicilio del área que está a cargo del tratamiento a auditar.

Cuando el responsable solicite que sea auditado **más de un tratamiento o área**, la **DGPAR determinará la procedencia de auditar todos los tratamientos o áreas en una misma auditoría**, o si es pertinente atenderlos en **diversas auditorías**, la determinación al respecto será informada al responsable solicitante.

NUMERAL 14 LINEAMIENTOS
La denominación y el domicilio del responsable solicitante
Las personas autorizadas para oír y recibir notificaciones
La descripción del tratamiento de datos personales que se pretende someter a la auditoría voluntaria
Finalidades del tratamiento
El tipo de datos personales tratados
Las categorías de titulares involucrados
Las transferencias que, en su caso, se realicen
Las medidas de seguridad implementadas; la tecnología utilizada
Cualquier otra información relevante del tratamiento a auditar (en su caso)
Las circunstancias o razones que lo motivan a someterse a una auditoría voluntaria
El nombre, cargo y firma de quien solicite la auditoría voluntaria. **Podrá ser:** ● **El titular de la dependencia o entidad u homólogo.** ● **El titular de la unidad administrativa u homólogo que será auditada.** ● **El Oficial de Protección de Datos Personales del responsable.** ● **El Presidente del Comité de Transparencia**
Cualquier otra información o documentación que considere relevante hacer del conocimiento del Instituto.
Denominación y domicilio del área que está a cargo del tratamiento a auditar.

Lista de comprobación y requisitos

Puede consultar la lista de comprobación que se aplica como referencia en el seguimiento y revisión de las Auditorías Voluntarias. Cabe señalar que deberán ser consideradas de manera enunciativa más no limitativa, dependiendo el tipo de tratamiento y alcance de la auditoria voluntaria. A continuación, podrá consultar los requerimientos de cada uno de los principios, deberes y obligaciones:

PRINCIPIO	DEBER	OBLIGACIONES
Responsabilidad	Seguridad	Transferencias
Proporcionalidad	Confidencialidad	Relación con encargados y cómputo en la nube
Licitud		Portabilidad
Lealtad		Evaluación de impacto
Información		Comité y unidad de transparencia
Finalidad		Capacitación
Consentimiento		Atención a derechos ARCO
Calidad		
DESCARGAR	DESCARGAR	DESCARGAR

Beneficios de una Auditoría Voluntaria

- Determinar el nivel de cumplimiento de la LGPDPPSO.
- Determina la eficacia de las medidas, controles y mecanismos implementados.
- Identifica oportunidades de mejora.
- Recomienda acciones preventivas y correctivas.
- Contribuye al cumplimiento del principio de responsabilidad.
- Con la mejora y corrección de los hallazgos, se podría evitar sanciones derivadas de alguna verificación.

Causales de improcedencia

- El Instituto tenga conocimiento de una denuncia en materia de protección de datos personales en contra del sujeto obligado, se esté sustanciando un procedimiento de verificación relacionado con el tratamiento a auditar.
- El sujeto obligado se encuentre seleccionado de oficio para ser verificado por parte del Instituto.
- El Instituto no sea competente.
- Se encuentre en trámite una solicitud idéntica por parte del mismo sujeto obligado;
- El área para auditar no forma parte del solicitante, o
- No se trate de una solicitud de auditoría en materia de protección de datos personales.

ESQUEMAS DE MEJORES PRÁCTICAS EN PROTECCIÓN DE DATOS PERSONALES

8. ESQUEMAS DE MEJORES PRÁCTICAS EN PROTECCIÓN DE DATOS PERSONALES

Las Mejores Prácticas en materia de protección de datos personales se enfocan en identificar acciones, reglas, criterios y procedimientos que resultan eficaces para elevar el nivel de protección de datos personales a través de acciones preventivas en la materia.

El objetivo de las Mejores Prácticas en materia de protección de datos personales permitirá a los responsables o encargados demostrar el cumplimiento que establece la Ley General mediante la adopción de Esquemas de Mejores Prácticas a los que refieren los artículos 72 y 73 de la Ley General y 119 de los Lineamientos.

Los Esquemas de Mejores Prácticas se definen como aquellas acciones, reglas, criterios y procedimientos que tienen como finalidad:

- Elevar el nivel de protección de los datos personales en el sector público.
- Armonizar el tratamiento de datos personales en un sector específico.
- Facilitar el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales a los titulares.
- Facilitar las transferencias de datos personales.
- Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales en el sector público.
- Demostrar ante el Instituto y otros interesados, el cumplimiento de la normatividad aplicable en materia de protección de datos personales en el sector público.

Los responsables o encargados podrán adoptar o desarrollar Esquemas de Mejores Prácticas (EMP) de manera individual o en acuerdo con otros responsables o encargados, y una vez que cuenten con la validación por parte del Instituto o de los órganos garantes locales, podrán ser Inscritos en el Registro de Esquemas de Mejores Prácticas (REMP)[20], para ello, previamente deberá cumplir con la normativa correspondiente a los Parámetros de Mejores Prácticas en materia de protección de datos personales del sector público (Parámetros)[21] y las Reglas de Operación del Registro de Esquemas de Mejores Prácticas (Reglas)[22].

Los EMP podrán tener un alcance total, cuando abarquen todos los principios, deberes y obligaciones previstos en la Ley General y demás normativa que de ella derive, incluyendo, en su caso, las reglas para adaptar la normativa, entre ellos, los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; los deberes de seguridad y confidencialidad, así como las obligaciones vinculadas a los derechos de los titulares, la relación entre responsable y encargado, las transferencias, las evaluaciones de impacto en la protección de datos personales y el establecimiento de un sistema de gestión de seguridad de datos personales, entre otros.

Así mismo, los EMP tendrán un **alcance parcial** cuando abarquen solo alguno o algunos principios, deberes y obligaciones previstos en la Ley General y demás normativa que de ellas derive, incluyendo, en su caso, las reglas para adaptar la normativa, entre ellos, los

[20]Consulta en: https://registro-esquemas.inai.org.mx/?page_id=610

[21]Consulta en: https://www.dof.gob.mx/2019/INAI/ACT-PUB-11-09-2019-07.pdf

[22]Consulta en: http://www.dof.gob.mx/2020/INAI/ACT-PUB-17-06-2020-04.pdf

principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; los deberes de seguridad y confidencialidad, así como las obligaciones vinculadas a los derechos de los titulares, la relación entre responsable y encargado, las transferencias, las evaluaciones de impacto en la protección de datos personales y el establecimiento de un sistema de gestión de seguridad de datos personales, entre otros.

Alcance material. A su vez, es importante que los esquemas de mejores prácticas determinen el alcance material considerando lo siguiente:

- **Total:** Cuando abarquen todos los procesos de datos personales que realice el responsable o encargado adherido.

- **Parcial:** Cuando abarquen sólo uno o algunos procesos específicos que realice el responsable o encargado adherido.

Registro de Esquemas de Mejores Prácticas (REMP).

El objeto del REMP, es organizar, administrar, gestionar, facilitar el acceso y difundir información de interés general relacionada con las modalidades de esquemas de mejores prácticas.

¿Cómo puedo inscribirme en el REMP?

Una vez que cumpla con lo establecido en los Parámetros y Reglas de Operación de acuerdo con la modalidad que prefiera, podrá solicitar la validación del esquema de mejores prácticas al Instituto, o en su caso a los órganos garantes locales, una vez que se cuente con dicha validación, se procederá a inscribir en el REMP y se le otorgará el distintivo REMP-INAI[23].

Imagen del Registro de Esquemas de Mejores Prácticas

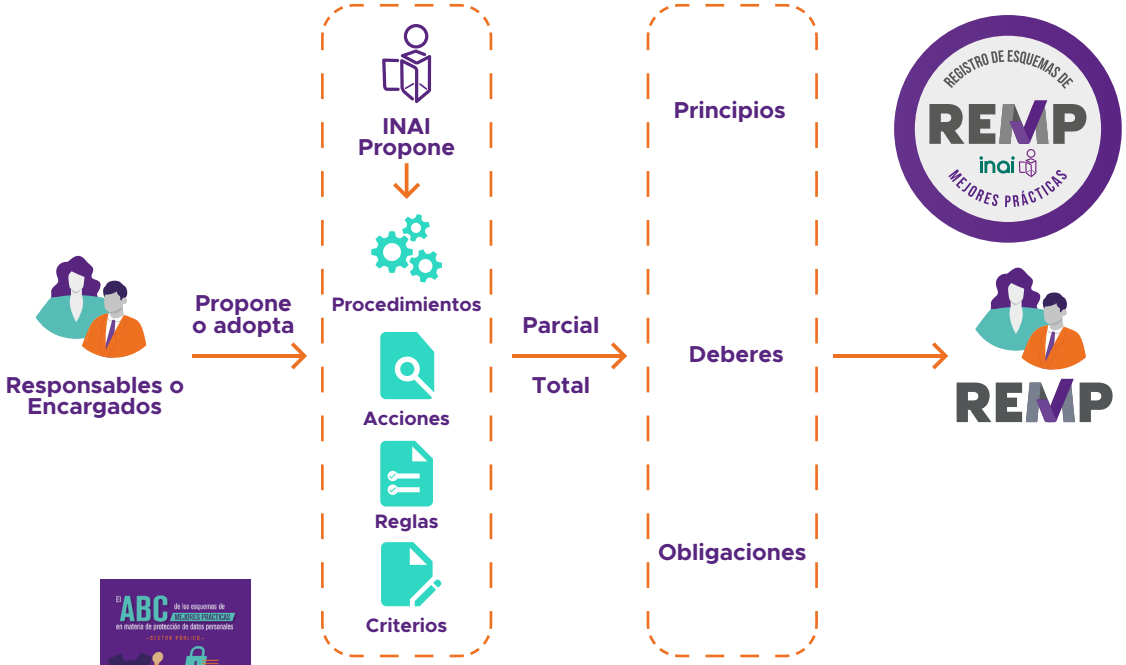
[23]Consulta en: https://registro-esquemas.inai.org.mx/wp-content/uploads/2022/11/Manual_de_uso_REMP-1.pdf

Modalidades de esquemas

-Reglas para adaptar normativa

Este tipo de esquema puede ser desarrollado por un responsable o encargado de un sector específico, o bien pueden ser propuestas por el Instituto. Las reglas deberán contener criterios, procedimientos, requisitos que permitan mejorar la eficacia de la implementación de principios, deberes y obligaciones en materia de protección de datos personales. Lo anterior, considerando la naturaleza, necesidades y características del sector en el cual se están desarrollando.

El Instituto podrá proponer a los responsables el desarrollo o adopción de Reglas para adaptar la normativa, cuando considere que ayudará a mejorar la eficiencia de la aplicación de la norma y podrán desarrollarse a través de códigos de buenas prácticas, modelos en materia de datos personales, programas u otros. A continuación, se muestra de manera general el proceso de adopción o desarrollo:



Puede consultar todo el procedimiento en el ABC de los esquemas de mejores prácticas en materia de protección de datos personales.

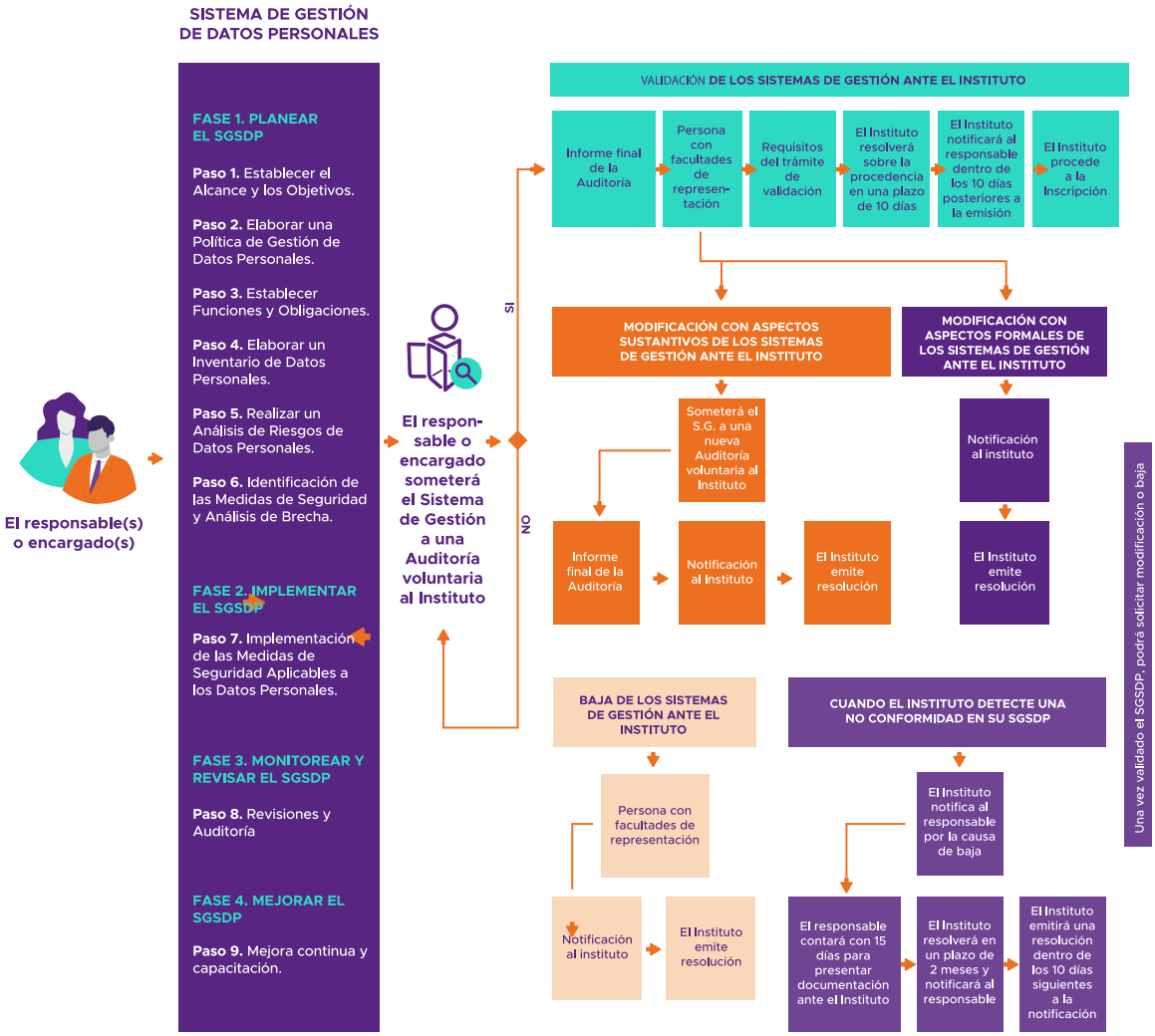
-Sistemas de Gestión validados

En el sector público la implementación de un Sistema de Gestión es obligatorio, según lo establecido en el artículo 34 de la Ley General y 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos).

De forma particular un Sistema de Gestión de Seguridad de Datos Personales (SGSDP) tiene por objetivo proveer un marco de trabajo para el tratamiento de datos personales, que permita mantener vigente y mejorar la protección de datos personales para el cumplimiento de la legislación y fomentar las buenas prácticas.

Es responsabilidad de los Sujetos Obligados que, su Sistema de Gestión contenga todas aquellas actividades que permiten establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en el artículo 34 de la Ley General.

A continuación, se muestra el diagrama general de los procedimientos para la validación, modificación o baja de los Sistemas de Gestión validados por el instituto.



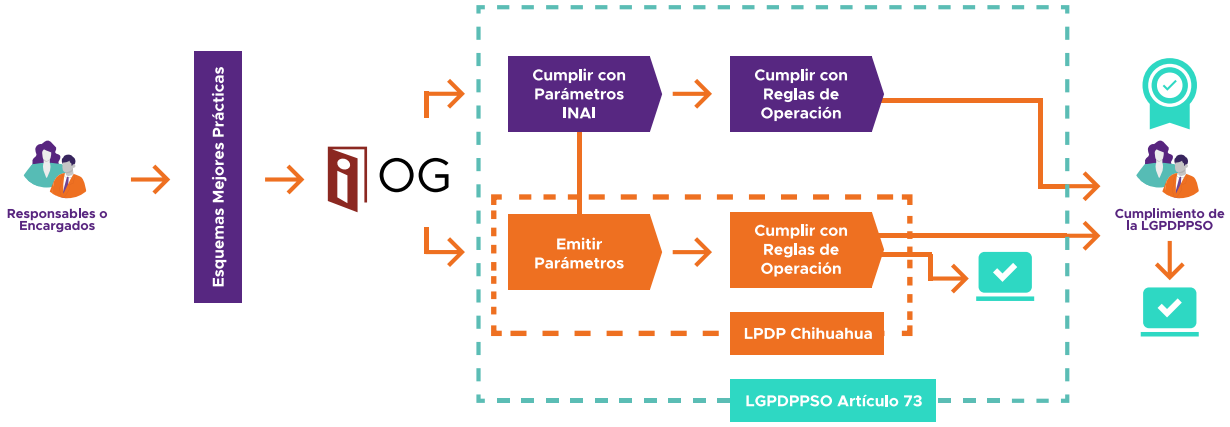
Puede consultar todo el procedimiento en el ABC de los esquemas de mejores prácticas en materia de protección de datos personales.

LOS ÓRGANOS GARANTES Y LAS MEJORES PRÁCTICAS

Es importante señalar que los Parámetros emitidos por el Instituto podrán servir de referente para que los órganos garantes locales emitan, si así lo consideran, sus propios parámetros y registro de mejores prácticas en materia de protección de datos personales de las entidades federativas. En caso de que algún órgano garante lo decida, podrán solicitar la inscripción de esquemas que fueron validados en el REMP, de acuerdo con los plazos y requerimientos establecidos en la normativa aplicable.

Puede consultar aquí a los **órganos garantes** locales que cuentan con normativa en materia de Mejores Prácticas en la Protección de Datos Personales.

A continuación, se muestra un ejemplo de cómo podrán operar los órganos garantes el sistema de esquemas de mejores prácticas:



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