inai

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

GUÍA para el Tratamiento de Datos Biométricos

Directorio

Francisco Javier Acuña Llamas
Comisionado Presidente

Areli Cano Guadiana
Comisionada

Oscar Mauricio Guerra Ford
Comisionado

María Patricia Kurczyn Villalobos
Comisionada

Rosendoevgueni Monterrey Chepov
Comisionado

Ximena Puente de la Mora
Comisionada

Joel Salas Suárez
Comisionado

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

Edición • Marzo 2018

Contenido

1. Glosario

Biometría[1]	Método de reconocimiento de personas basado en sus datos biométricos.
Criterios	Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos.
Dato biométrico[2]	Propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.
Disposiciones	Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.
INAI o Instituto	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
LFPDPPP o Ley Federal	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
LGPDPPSO o Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Lineamientos	Lineamientos del Aviso de Privacidad.
Lineamientos Generales	Lineamientos Generales de Protección de datos Personales para el Sector Público.

[1] Definición integrada a partir de lo señalado en el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 y el Documento Privacy & Biometrics. Building a conceptual foundation. National Science and Technology Council. Committee on Technology. Committee on Homeland and National Security, Subcommittee on Biometrics, Estados Unidos, 2006.

[2] Definición integrada a partir de lo señalado en el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 y el Documento Privacy & Biometrics. Building a conceptual foundation. National Science and Technology Council. Committee on Technology. Committee on Homeland and National Security, Subcommittee on Biometrics, Estados Unidos, 2006.

Lineamientos de Portabilidad	Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales.
Muestra biométrica	Prototipo de un dato biométrico.
Parámetros	Parámetros de Autorregulación en materia de Protección de Datos Personales.
Plantilla biométrica	Representación alfanumérica de la información extraída de una o más muestras biométricas.
Reconocimiento biométrico	Identificación o verificación de la identidad de una persona a partir de la comparación de platillas biométricas.
Registro	Proceso de recolección de muestras biométricas y su ingreso a un sistema biométrico, para su posterior comparación.
RLFPDPPP o Reglamento de la Ley Federal	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Sistemas biométricos[3]	Son las aplicaciones tecnológicas que permiten el reconocimiento automático de una persona a través de sus datos biométricos.

[3] Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 y Documento Privacy & Biometrics. Building a conceptual foundation. National Science and Technology Council. Committee on Technology. Committee on Homeland and National Security, Subcommittee on Biometrics, Estados Unidos, 2006.

2. Introducción

El imparable desarrollo tecnológico ha facilitado, de formas antes impensables nuestras actividades cotidianas, un ejemplo de ello es el uso de nuestros biométricos. Cada vez es más frecuente que nuestra huella digital, iris o voz, sea la llave de entrada a nuestro lugar de trabajo, computadora o teléfono celular.

En el mismo sentido, nuestra información biométrica puede ser utilizada por las autoridades para cumplir de mejor manera con sus facultades y para proveer mejores servicios a la ciudadanía, por ejemplo, en los procesos de reposición de documentos de identificación, de control migratorio, o en el ámbito penal.

Como veremos más adelante, los datos biométricos, como regla general, se pueden considerar datos personales. Por ello, las empresas, organizaciones, profesionistas y autoridades deben realizar el tratamiento de esta información bajo las condiciones que establece la normativa en la materia.

Para apoyar en esta labor, el INAI elaboró la presente guía, dirigida a los responsables o encargados de los sectores público y privado, que pretendan o traten en la actualidad datos biométricos a través de medios digitales o electrónicos, es decir automatizados, con el objeto de que el tratamiento se realice de conformidad con los principios, deberes y obligaciones establecidas en la LFPDPPP y en la LGPDPPSO, así como demás normativa aplicable. [4]

El documento incluye un glosario que facilita el entendimiento de los términos técnicos más relevantes utilizados en la guía. Igualmente, contiene un apartado donde se describen las características y generalidades de los datos biométricos y, en especial y dada su amplia utilización, de la huella dactilar.

Como parte fundamental de la guía está el apartado que explica los casos en los que un dato biométrico es considerado como un dato personal.

[4] En el caso de instituciones públicas estatales o municipales, para el debido tratamiento de datos biométricos, éstas deberán observar, de manera adicional, las disposiciones locales existentes en la materia.

Una vez que se ha explicado qué es un dato biométrico y sus características, y que se ha expuesto cuándo se puede considerar dato personal, la guía desarrolla el apartado de recomendaciones de la siguiente forma:

- Brinda una breve explicación de los conceptos fundamentales para entender el derecho de protección de datos personales;
- Proporciona una descripción detallada de cada uno de los principios, deberes y derechos previstos por la normativa en materia de protección de datos personales;
- Identifica y explica las obligaciones vinculadas con cada uno de ellos, y
- Desarrolla las recomendaciones para que en el tratamiento de datos biométricos se cumplan las obligaciones previamente descritas.

Finalmente, la guía enlista las fuentes principalmente consultadas para su elaboración, para mayor referencia y por si el usuario quiere profundizar en el conocimiento de este tema.

Esperamos que esta guía le sea de utilidad.

3. Los datos biométricos

A) Qué son y cuáles son sus características principales

De acuerdo con la definición contenida en el glosario de esta guía, los datos biométricos son las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.[5]

De conformidad con el Grupo de trabajo del Artículo 29, los datos biométricos, en mayor o menor medida, son:[6]

1. **Universales**, ya que son datos con los que contamos todas las personas;
2. **Únicos**, ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas;
3. **Permanentes**, ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona, y
4. **Medibles** de forma cuantitativa.

Entre los datos biométricos que refieren a características físicas y fisiológicas se encuentran la huella digital, el rostro (reconocimiento facial), la retina, el iris, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, la piel o textura de la superficie dérmica, el ADN, la composición química del olor corporal y el patrón vascular, pulsación cardíaca, entre otros.

[5] A modo de referencia, el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento Europeo), en su artículo 4, inciso 14, define como datos biométricos a los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

[6] Adicionalmente, existen varias formas en las que un dato biométrico puede presentarse y esto se encuentra vinculado a la cantidad de información que revelan. Atendiendo a lo anterior, se dice que un dato biométrico se presenta en su **imagen pura**, cuando es reconocible a simple vista como la imagen de una huella dactilar; que se presenta en una **imagen cifrada** cuando los datos sólo pueden ser recreados por ciertas personas o tecnologías para ser usados para generar una imagen; y que se presenta en una **imagen parcialmente cifrada**, cuando existen datos parciales de una imagen, los cuales son cifrados, y no pueden ser usados para recrear la imagen completa original.

Por otro lado, entre los datos biométricos que refieren a las características del comportamiento y los rasgos de la personalidad se encuentran la firma autógrafa, la escritura, la voz, la forma de oprimir un teclado y la forma de caminar, entre otros.

El tipo de dato biométrico determinará el sistema biométrico a ser utilizado para el reconocimiento de la persona. Es pertinente señalar que cada sistema biométrico tiene sus características propias.

Las tecnologías biométricas de reconocimiento de características físicas y fisiológicas consideran parámetros derivados de la medición directa de algún rasgo estrictamente físico o funcional del cuerpo humano a la hora de identificar personas. Entre las más comunes se encuentran:

Biométrico	Descripción de reconocimiento
Huella dactilar	Es la más antigua y existen dos técnicas: (i) Basada en minucias y (ii) basada en correlación. Esta última requiere un registro más preciso pues se analiza el patrón global seguido por la huella dactilar.
Reconocimiento facial	El análisis se realiza a través de mediciones como la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula.
Reconocimiento de iris	Una cámara infrarroja escanea el iris y proporciona sus detalles. Los patrones del iris vienen marcados desde el nacimiento y rara vez cambian, son muy complejos y contienen una gran cantidad de información, más de 200 propiedades únicas.
Geometría de la mano	A través de una cámara se captura imágenes en 3-D, se extraen características que incluyen las curvas de los dedos, su grosor y longitud, la altura y la anchura del dorso de la mano, las distancias entre las articulaciones y la estructura ósea.
Reconocimiento de retina	Se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma. Cada patrón es único incluso entre los gemelos idénticos y tiene una tasa de falsos positivos prácticamente nula.
Reconocimiento vascular	Se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo. Es interno y no deja rastro por lo que el robo de identidad es muy difícil.

Por su parte, las tecnologías biométricas de reconocimiento de características del comportamiento y la personalidad se caracterizan por considerar en el proceso de identificación rasgos derivados de una acción realizada por una persona. Entre las más comunes se encuentran:

Biométrico	Descripción de reconocimiento
Reconocimiento de firma	Analiza la firma autógrafa o manuscrita para confirmar la identidad del firmante. Existen dos variantes: (i) Comparación simple, que considera el grado de parecido entre dos firmas, y (ii) verificación dinámica, que hace un análisis de la forma, velocidad, presión de la pluma y la duración del proceso de firma.
Reconocimiento de escritura	Se vale de un software de reconocimiento de caracteres, atendiendo a que cada persona tiene una forma de escribir diferente, teniendo rasgos propios e inconfundibles para cada letra. De igual forma, cada persona tiene un grado de inclinación y nivel de presión al escribir.
Reconocimiento de voz	Se usan sistemas de inteligencia artificial con algoritmos que deben medir y estimar la similitud entre las muestras para devolver un resultado o una lista de posibles candidatos.

Biométrico	Descripción de reconocimiento
Reconocimiento de escritura de teclado	Se basa en el hecho de la existencia de un patrón de escritura en el teclado permanente y propio de cada individuo, por lo que un software mide la fuerza de tecleo, la duración de la pulsación y el periodo que pasa entre que se presiona una tecla y otra.
Reconocimiento de la forma de andar	Se graba la forma de caminar de una persona y se somete a un proceso analítico que genera una plantilla biométrica única. Se encuentra aún en desarrollo y no tiene los mismos niveles de rendimiento que otras tecnologías biométricas.

Es importante señalar que a pesar de que los datos biométricos son relativamente efectivos para distinguir individuos, éstos tienen distintos grados de estabilidad, por ejemplo, las huellas dactilares y el iris tienden a mantenerse estables a través del tiempo y son difíciles de alterar, mientras que el rostro puede modificarse con el tiempo y disimularse mediante el uso de cosméticos, disfraces, cirugías y hasta con posturas y muecas.

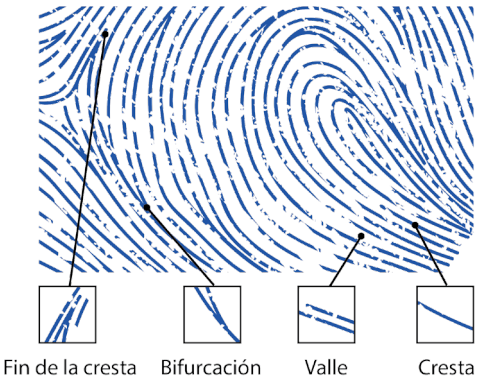
B) Las huellas dactilares

Los sistemas biométricos de reconocimiento de huellas dactilares son los más comúnmente utilizados debido a lo fácil que resulta recolectar de las personas este dato.

Las huellas dactilares se forman a partir de la superficie desigual de la piel de los dedos de la mano, en donde se identifican diversas protuberancias y hendiduras conocidas como crestas y valles, las cuales se encuentran dispuestas de modo único.

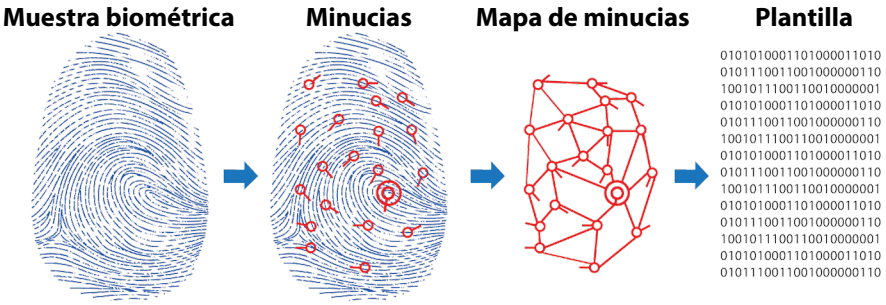
Si bien a una huella dactilar se le pueden aplicar procedimientos manuales de reconocimiento biométrico conocidos como técnica biométrica de correlación, la presente guía se enfocará a la técnica biométrica automatizada basada en minucias.

Cuando se registra una huella dactilar en un sistema de reconocimiento, ésta aparece como una serie de líneas oscuras que representan las crestas y de líneas blancas que representan los valles, ubicados entre las crestas. A menudo, las crestas son más cortas y se detienen y comienzan abruptamente. Esta combinación de crestas y valles, con sus correspondientes ubicaciones, direcciones, bifurcaciones, inicios y finales -las minucias-, resultan en un patrón único de características de cada huella dactilar. Las minucias son, entonces, aquellos puntos de interés en toda huella digital.



Fuente: GAO adaptación de datos del FBI

La información de las minucias -principalmente las bifurcaciones y las terminaciones de las crestas, aunque también se utilizan otras minucias- es la que se recolecta y la que posteriormente se utiliza para desarrollar la plantilla.



Uno de los componentes esenciales en el campo del reconocimiento de huellas dactilares, es el desarrollo de estándares técnicos. Este enfoque es manejado por la vasta variedad de algoritmos y sensores disponibles en el mercado. La interoperabilidad está relacionada con los estándares de la tecnología y es otro aspecto crucial en la implementación del producto. Las plantillas generadas por un sistema biométrico para reconocimiento dactilar deberían ser capaces de ser interpretadas por otra computadora usando un sistema diferente.

Cabe señalar que, de acuerdo con el análisis de los sistemas biométricos para reconocimiento dactilar, realizado por NIST,[7] derivado de la USA PATRIOT ACT, en donde se evaluó la precisión de distintos sistemas de esta clase, se concluyó que la utilización de cuatro a diez huellas dactilares resulta tan eficiente como la utilización de una sola huella dactilar de alta calidad.

C) El reconocimiento de las personas a través de un dato biométrico

El objeto del sistema biométrico es reconocer a las personas, es decir, "volver a conocer" a una persona que ha sido identificada y registrada previamente. En otras palabras, el reconocimiento implica comparar –de manera manual o automatizada- una muestra biométrica de una persona con plantillas previamente registradas y relacionadas con una identidad específica.

Los datos biométricos en la vida diaria

Uno de los usos más frecuentes de los datos biométricos es el que se realiza en los lugares de trabajo, para **controlar la asistencia** de los empleados o para asegurar que sólo las personas autorizadas ingresen a determinada zona del lugar de trabajo; pero también pueden usarse como **medio para acceder a determinadas aplicaciones o dispositivos** como la computadora o el celular.

Igualmente, los biométricos son utilizados para robustecer el **control migratorio** y, en el ámbito penal, para que la autoridad confirme la **identidad de un imputado a una infracción**, entre otros usos. Asimismo, con mayor frecuencia, los datos biométricos se utilizan para confirmar la identidad del individuo en las **transacciones financieras**, para evitar daños patrimoniales o jurídicos.

[7] Instituto Nacional de Estándares de los Estados Unidos de América (NIST, por sus siglas en inglés)

El reconocimiento de los individuos puede llevarse a cabo a través de los procesos de identificación o de verificación.

La identificación[8] consiste en comparar la muestra biométrica recolectada de una persona frente a una base completa de datos biométricos registrados previamente. No se requiere de ningún dato adicional del usuario, es decir, el único dato que se recoge en el momento del uso es una muestra biométrica, sin apoyo de un nombre de usuario u otro dato, la cual es transformada en plantilla. Por ejemplo, una base de datos de criminales, donde se compara uno o más datos biométricos **contra todos los registros** de una base de datos en posesión de la policía a fin de encontrar una coincidencia.

Dicho método requiere de un proceso de cálculo complejo, puesto que se ha de comparar esta nueva plantilla con cada una de las plantillas anteriormente almacenadas y relacionadas a personas específicas para buscar una coincidencia (comparación uno a muchos, 1:N).

Este proceso permite determinar: i) si en la base de datos biométricos de determinado sistema biométrico existe una muestra coincidente y ii) en caso de que así sea, la identidad de la persona. Por ejemplo, un nombre o número vinculado a dicha plantilla.

La precisión de un sistema biométrico de identificación puede medirse a través de las siguientes formas: i) tasa de falsa alarma, es decir, la tasa en la que un sistema biométrico realiza coincidencias de plantillas de manera incorrecta, determinando que una persona es quien no es en realidad y ii) tasa de identificación, es decir, la tasa de coincidencias –identificaciones- realizadas correctamente.

La **verificación** es un método cuyo primer paso es la individualización del usuario mediante algún nombre, tarjeta, dispositivo inteligente o algún otro método, y la obtención de su muestra biométrica la cual es convertida en una plantilla. Posteriormente, se realiza la selección de la plantilla anteriormente registrada para dicho usuario. Por último, se comparan ambas plantillas (comparación uno a uno, 1:1), se determina si son coincidentes y, en ese sentido, si la persona es o no quien dice ser, es decir, el resultado es positivo si las plantillas coinciden o negativo si no lo hacen. Este proceso es simple, al tener que comparar únicamente dos plantillas.

Como ejemplos de este método, están los registros de asistencia, donde se compara uno o más datos biométricos **contra el mismo registro** almacenado para comprobar que un empleado es quien dice ser, o bien **la verificación de la huella dactilar de un usuario** para desbloquear su teléfono inteligente.

La precisión de un sistema biométrico de verificación puede medirse de las siguientes formas: i) tasa de falsos positivos, es decir, la tasa de verificaciones incorrectas porque se determine que una persona es quien dice ser cuando en realidad no lo sea, ii) tasa de falsos negativos, es decir, la tasa de verificaciones incorrectas porque se determine que una persona no es quien dice ser cuando en realidad sí lo sea, y iii) tasa de verificación, es decir, la tasa de coincidencias –verificaciones- realizadas correctamente.

Visto lo anterior, es posible identificar las siguientes fases de los sistemas biométricos, tanto de verificación como de identificación. Dichas fases implican distintos tratamientos de datos personales:

[8] Tal y como se señala en el estudio sobre Privacidad y Biométricos del Consejo Nacional de Ciencia y Tecnología de Estados Unidos, la identificación de las personas que se realiza a través de estos sistemas biométricos de identificación (identificación por sistema) es distinta –y más limitada- a la identificación que una persona tiene fuera del sistema biométrico (identificación absoluta). Al respecto, se entiende que esta otra identificación fuera del sistema está relacionada a cuestiones jurídicas o de hecho, por ejemplo, al nombre con el que una persona es registrada en el Registro Civil o el nombre con el que la gente de su comunidad lo reconoce.

1. **Registro.** Es el primer paso de un sistema biométrico y se realiza a través de sensores o aparatos que observan y graban ciertas muestras biométricas. Abarca tanto la recolección de la muestra como su ingreso al sistema.
2. **Conversión.** Es el proceso por el cual se convierte la muestra biométrica recopilada en una plantilla.
3. **Almacenamiento.** Proceso por el que se guardan las plantillas generadas durante la fase de recolección y durante el proceso de verificación o identificación.[9]
4. **Comparación.** La plantilla nueva (obtenida de la "captura en vivo") es comparada con la(s) otra(s) plantilla(s) generadas y guardadas previamente, a través de cálculos algorítmicos y de puntajes de coincidencia que se evalúan con base en umbrales de coincidencia previamente establecidos.[10]
5. **Decisión.** Consiste en el proceso a través del cual se toma una decisión de forma automática o con asistencia humana sobre la verificación o identificación basada en el resultado de la fase de comparación. Esta decisión es comunicada por el sistema biométrico al usuario que puede ser el propio sujeto a identificarse o verificarse, o bien, un tercero.

Aunado a la variabilidad en la estabilidad de los distintos datos biométricos, un sistema biométrico sólo es tecnológicamente capaz de determinar dentro de una probabilidad estadística si la plantilla analizada coincide o no con las plantillas previamente almacenadas. En este sentido, los sistemas biométricos no pueden garantizar una exactitud completa.

Por ello, tanto la gestión, supervisión y evaluación de los efectos de un sistema biométrico deberían considerar siempre la naturaleza probabilística del proceso e integrar dicha característica en las políticas y procedimientos del uso del sistema. Como ya vimos, esto puede hacerse a través de estadísticas como las tasas de verificaciones o de verificaciones incorrectas y las tasas de falsa alarma –o falso positivo- y de identificación.

Es importante señalar que los procesos de reconocimiento biométrico pueden ser automatizados, semiautomatizados, y manuales, lo que implica que pueden involucrar ciertas etapas de recolección o análisis donde intervenga el factor humano.

Ahora bien, aunque el uso de datos biométricos para identificar o verificar la identidad de una persona es cada vez más común, éstos **no son la única alternativa para llevar a cabo el proceso de reconocimiento**.

En general, existen tres factores a partir de los cuales se puede identificar o verificar la identidad de una persona:

1) A través de algo que la persona **sabe**, por ejemplo, una contraseña o código PIN.
2) A partir de algo que la persona **posee**, por ejemplo, una tarjeta de proximidad o un token.
3) Por medio de algo que la persona es, por ejemplo, un dato biométrico.

[9] Este almacenamiento puede hacerse en una base de datos que contenga todas las muestras y plantillas biométricas obtenidas, o bien, en una tarjeta inteligente que contenga sólo la muestra o plantilla biométrica del dueño del dato biométrico y usuario de dicha tarjeta.

[10] Establecer el umbral de coincidencia no es una tarea sencilla ya que, por ejemplo, las tasas de verificación, de falsos negativos y de falsos positivos son variables dependientes y si el umbral de coincidencia se fija en un valor bajo, la tasa de tasa de verificación aumentará y la tasa de falsos negativos disminuirá, pero, en el mismo sentido, la tasa de falsos positivos aumentará.

Para determinar cuál de los tres factores de reconocimiento es el adecuado para identificar o verificar la identidad de una persona en un tratamiento en lo particular, se deben tomar en cuenta diversos criterios, como los siguientes:[11]

Comparación de los factores de reconocimiento			
Criterios	**Algo que la persona es (dato biométrico)**	**Algo que la persona posee (token o tarjeta de proximidad)**	**Algo que la persona sabe (contraseña o PIN)**
Menor necesidad de secreto	No es necesario que el titular mantenga en secreto u ocultos sus datos biométricos, aunque el responsable deba resguardarlos con las medidas de seguridad óptimas.	Las tarjetas o el token no deben estar al alcance de todos.	Las contraseñas deben ocultarse.
Menor posibilidad de robo	El robo de un dato biométrico y la posibilidad de su uso posterior es más complicado que los otros dos elementos.	El robo del token o tarjetas de proximidad no es poco común ni difícil.	Un descuido del titular puede dar lugar al robo o acceso no autorizado de su contraseña.
Menor posibilidad de pérdida	Al dato biométrico es, en general, permanente y siempre acompaña a la persona.	Las tarjetas y token se pueden perder con facilidad.	El olvido de contraseñas es común.
Fácil registro inicial y posibilidad de renovación	La generación de registros biométricos es más complicada por las distintas fases que conlleva, además que los datos biométricos son limitados.	La facilidad de emitir una tarjeta de proximidad o token es relativamente sencilla comparada con la generación de un registro biométrico.	La facilidad de emitir contraseñas es relativamente sencilla comparada con la generación de un registro biométrico. Además, la capacidad de generar datos biométricos es limitada, mientras que ello no ocurre con las contraseñas.
Fácil proceso de comparación	La comparación de datos biométricos es mucho más complicada, por el procesamiento y capacidades tecnológicas que requiere.	La comparación de tarjetas o token también puede ser sencilla.	La comparación de contraseñas es sencilla.
Mayor comodidad de uso	Como ya se ha dicho, el dato biométrico acompaña a su titular y en general es permanente.	Las tarjetas o token se deben tener a la mano.	Las contraseñas se deben memorizar o gestionar con un programa de administración de contraseñas.
Menor vulnerabilidad a la ingeniería social y ataques técnicos	Si bien los sistemas biométricos pueden ser vulnerados, es más complicado que ello ocurra y que los datos biométricos puedan ser reutilizados, y serán aún más complicado que se pueda vulnerar al propio titular para obtener sus biométricos.	Se puede utilizar ingeniería social o engaño para robar o duplicar una tarjeta o token.	Se puede utilizar ingeniería social, espionaje, engaño o fuerza bruta para obtener de manera ilegítima una contraseña.

[11] Tecnologías biométricas aplicadas a la ciberseguridad, España, INCIBE, 2016. Consultable en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Criterios	Algo que la persona es (dato biométrico)	Algo que la persona posee (token o tarjeta de proximidad)	Algo que la persona sabe (contraseña o PIN)
Mayor madurez en medidas de prevención	Las medidas de prevención de los sistemas biométricos no cuentan con el mismo nivel de madurez.	Los ataques a sistemas que utilizan tarjetas o token ocurren desde hace muchos años, por lo que las medidas de prevención presentan un grado de madurez importante.	Los ataques a sistemas que utilizan contraseñas ocurren desde hace muchos años, por lo que las medidas de prevención presentan un grado de madurez importante.
Mejor autenticación de usuarios reales	El dato biométrico, al pertenecer a un individuo en particular, no puede ser compartido ni transferido.	La autenticación de usuarios mediante tarjetas o token depende de hacer estos elementos intransferibles.	La autenticación de usuarios mediante contraseñas depende, en gran medida, de la voluntad de los usuarios de hacer estos elementos únicos.
Menor costo de implementación	Un sistema biométrico puede ser relativamente más costoso que un lector de tarjetas o un sistema de contraseñas, aunque en un análisis más profundo de costo-beneficio pueda resultar ventajoso.	Instaurar un sistema lector de tarjetas puede ser relativamente más barato que la implementación de un sistema biométrico.	Instaurar un sistema de contraseñas puede ser relativamente más barato que la implementación de un sistema biométrico.
Menor costo de mantenimiento	El costo de mantenimiento de un sistema biométrico, una vez que está implementado, puede ser menor al de un sistema de contraseñas o tarjetas, ya que no conlleva gastos de gestión o reposición.	El costo de mantenimiento de un sistema biométrico, una vez que está implementado, puede ser menor al de un sistema de tarjetas, ya que no conlleva gastos de gestión o reposición.	El costo de mantenimiento de un sistema biométrico, una vez que está implementado, puede ser menor al de un sistema de contraseñas ya que no conlleva gastos de gestión.

Como se puede observar, ninguno de los tres elementos tiene por sí mismo todas las ventajas o desventajas asociadas a los factores antes mencionados. En ese sentido, resulta recomendable utilizar un factor de reconocimiento múltiple, adaptado a las circunstancias concretas del tratamiento en cuestión.

En el caso de los datos biométricos y sus sistemas, el factor de reconocimiento múltiple podría consistir en:

1) Biometría multimodal: Consiste en utilizar dos o más datos biométricos de manera conjunta. Este método se utiliza con la finalidad de aumentar la capacidad de reconocimiento de un sistema biométrico.
2) Reconocimiento multimodal: Consiste en utilizar un dato biométrico en combinación con una contraseña, pin, tarjeta o token. Este método puede tener dos finalidades: (i) reforzar la identificación o verificación de la identidad de la persona, al requerir dos o más elementos para comprobar la identidad y; (ii) que exista un método de verificación de respaldo en caso de falla o malfuncionamiento del sistema biométrico.

Concluimos este apartado señalando que la adquisición de determinado sistema biométrico es decisión del responsable, quien deberá considerar diversos factores como la naturaleza de sus actividades, la finalidad del tratamiento, la naturaleza del biométrico a utilizar, la interoperabilidad entre sistemas biométricos[12] y el costo.

[12] Los sistemas biométricos correspondientes a distintas clases de biométricos generalmente utilizan distintos métodos de obtención de muestras biométricas y no es posible utilizar las muestras obtenidas por un sistema biométrico en otro sistema biométrico salvo las huellas dactilares, en donde existen estándares (INCITS 378 o el ISO/IEC 19794-2:2005) que especifican las características que deben ser satisfechas por las plantillas biométricas de las huellas dactilares para que pueda existir interoperabilidad entre los distintos sistemas que utilizan este biométrico para reconocimiento.

4. ¿Cuándo un dato biométrico se considera dato personal?

Una vez que hemos descrito qué es un dato biométrico y cuáles son sus principales características, podremos definir las circunstancias bajo las cuales se podrán considerar un dato personal.

De acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los datos personales son cualquier información concerniente a una persona física **identificada o identificable**[13]. Lo anterior, independientemente de la forma en que dicha información se encuentre expresada, misma que pude ser numérica, alfabética, gráfica, fotográfica, acústica, entre otras.

Ambas leyes precisan que una persona es identificable cuando su identidad pueda determinarse, directa o indirectamente, a través de cualquier información.

A partir de la definición anterior, podemos observar que hay dos condiciones que se deben cumplir para que cierta información se considere un dato personal:

1. Debe referir a una persona física, y
2. Debe identificar o hacer identificable a su titular.

Como ya se ha señalado, los datos biométricos son las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles. En ese sentido, podemos concluir que cumplen con la primera condición antes descrita, pues refieren y están asociados a una persona física en lo particular.

En cuanto a la segunda condición, es decir, a que identifiquen o hagan identificable a su titular, se puede advertir que, si bien existen datos biométricos que por sí mismos identifican a una persona, por ejemplo, el rostro de una persona conocida; la mayoría de ellos requiere de un procesamiento o información adicional para que sea posible reconocer a su titular, como se explicó en la tercera sección de esta guía.

Tal es el caso de la huella digital, que por sí sola y de manera aislada no identifica a su titular, pero cuando ingresa a un sistema en el que se vincula a un individuo en lo particular y después se pueden comparar nuevas muestras con la plantilla previamente registrada, se vuelve un dato personal, al hacer identificable a su titular.

[13] A modo de referencia, se señala que el Reglamento Europeo prevé que una persona física es identificable cuando su identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

De hecho, como se ha explicado, en la actualidad, los datos biométricos son utilizados precisamente con el propósito de reconocer a los individuos y confirmar su identidad, mediante el uso de la tecnología y métodos científicos, que permiten recolectarlos, almacenarlos, compararlos e interpretarlos.

No obstante, un dato biométrico aislado, que no pueda ser registrado en un sistema biométrico, ni se pueda vincular con un sujeto en lo particular o comparar con otras muestras, no podría considerarse un dato personal, ya que, por una parte, por sí mismo no identificaría a su titular, y por la otra, los esfuerzos necesarios para hacerlo identificable serían desproporcionados.

Entonces, un dato biométrico será dato personal cuando de manera directa identifique a su titular, o bien, lo haga identificable a través de la biometría, pues sin la aplicación de este método serían desproporcionales los esfuerzos que se requerirían para reconocer a la persona.

Por otra parte, tanto la Ley General como la Federal contemplan una figura especial de datos personales, los denominados "datos personales sensibles", que se definen como aquéllos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Adicionalmente, se enlista una serie de datos personales que explícitamente son considerados como sensibles, incluyendo los que revelen aspectos como el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas o morales, las opiniones políticas, la preferencia sexual y, en el caso de la Ley Federal, la afiliación sindical.

Si bien los datos biométricos no están mencionados de manera expresa en el listado de datos personales sensibles que se incluyen en ambas leyes[14], ello no implica que no se puedan considerar como tales bajo ciertas circunstancias. Para determinar tal característica, se requiere atender las condiciones del caso concreto, a fin de analizar si los datos biométricos en cuestión actualizan alguno de los siguientes tres supuestos que prevén la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares para considerar un dato personal como sensible:

a) Que se refieran a la esfera más íntima de su titular;
b) Que su utilización indebida pueda dar origen a discriminación, o
c) Que su uso ilegítimo conlleve un grave riesgo para su titular.

Por ejemplo, el dato biométrico del iris podría considerarse sensible en los casos en que permita obtener información sobre el estado de salud de su titular. Asimismo, una huella digital podría considerarse sensible si a través de un uso indebido de la misma se puede tener acceso a información privilegiada que pudiera poner en riesgo la seguridad o estabilidad patrimonial o financiera de una persona o incluso su condición jurídica.

En los casos en los que un dato biométrico se considere sensible, se requerirá de una protección reforzada.

Una vez precisados los casos en los que un dato biométrico podrá considerarse personal y sensible, los siguientes apartados desarrollarán las recomendaciones específicas para que su tratamiento sea conforme a lo dispuesto por las normas que regulan la protección de datos personales en el sector público y privado.[15]

[14] Distinto de lo que sucede con nuestra legislación que no hace una mención explícita al respecto, el artículo 9, inciso 1, del Reglamento Europeo prevé que los datos biométricos dirigidos a identificar de manera unívoca a una persona física son considerados como datos con una categoría especial, es decir, datos sensibles.

[15] Por ejemplo, en la resolución ACT-PRIV-20/01/2016.03.01.01, el Pleno del INAI señaló que, en el caso concreto, las huellas digitales se consideran como datos personales sensibles.

5. Recomendaciones para el tratamiento de datos biométricos

5.1 Conceptos básicos para comprender el derecho de protección de datos personales

A continuación, se presentan las definiciones de aquellos conceptos que resultan claves para comprender el derecho de protección de datos personales:

- **Aviso de privacidad:** documento físico, electrónico o en cualquier otro formato, a través del cual el responsable informa al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, previo a que ocurra dicho tratamiento.
- **Datos personales:** cualquier información concerniente a una persona física, que la identifique o que la haga identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otra forma.
- **Datos personales sensibles:** aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Entre otros, se consideran sensibles aquéllos que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, preferencia sexual.[16]
- **Encargado:** persona física o moral ajena a la organización del responsable que, sola o conjuntamente con otras, trate datos personales por cuenta del responsable.
- **Responsable:** Para la LFPDPPP, es la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. Para la LGPDPPSO, los responsables son los sujetos obligados que deciden sobre el tratamiento de datos personales, incluida cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal.
- **Titular:** persona física a quien corresponden los datos personales.
- **Transferencia:** Toda comunicación de datos personales realizada a persona distinta del titular, el responsable o encargado del tratamiento.
- **Tratamiento:** obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

[16] Asimismo, de conformidad con el artículo 3, fracción VI, de la LFPDPPP, la afiliación sindical también es un dato personal sensible cuando está involucrado un tratamiento por parte de particulares.

5.2 ¿A quiénes aplica la regulación en materia de protección de datos personales?

Serán sujetos obligados en términos de la LFPDPPP, los particulares, sean personas físicas o morales, que lleven a cabo el tratamiento de datos personales, con excepción de: (i) las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables; y (ii) las personas que lleven a cabo el tratamiento de datos que sea para uso exclusivamente personales, y sin fines de divulgación o utilización comercial.

Por otro lado, de acuerdo a la LGPDPPSO, serán sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

En ese sentido, cualquier persona, empresa, organización o autoridad que trate datos biométricos y decida sobre dicho tratamiento, deberá atender cualquiera de las dos normativas mencionadas que le aplique y la que de ella derive, para lograr un adecuado tratamiento de dicha información.

5.3 Principios, deberes, derechos y prerrogativas que rigen la protección de datos personales

Con la entrada en vigor de la LFPDPPP, el 6 de julio de 2010, así como de la LGPDPPSO, el 27 de enero de 2017, se reconocen una serie de principios, deberes y derechos rectores de la protección de datos personales, de observancia obligatoria para los particulares y sujetos obligados del sector público que tratan datos personales, y que en su conjunto garantizan un adecuado manejo de los mismos, a favor de la privacidad y de la autodeterminación informativa de los titulares de los datos personales.

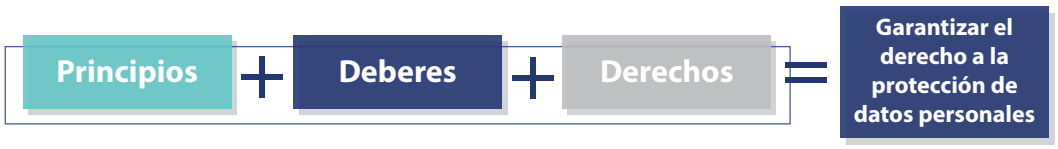
De acuerdo con las citadas leyes, los principios rectores de la protección de datos personales son:

Estos principios se traducen en obligaciones concretas para los responsables del tratamiento de los datos personales, las cuales se describirán a detalle en la siguiente sección.

De manera adicional, se reconocen los deberes de seguridad y confidencialidad, los cuales también establecen obligaciones concretas a quienes traten datos personales en el ejercicio de sus actividades.

Asimismo, los responsables del tratamiento deberán garantizar y facilitar a los titulares de los datos personales el ejercicio de los derechos de acceso, rectificación, cancelación, oposición (Derechos ARCO), la revocación del consentimiento y la prerrogativa de portabilidad[17].

En suma:



Tomando en cuenta lo anterior, en el siguiente apartado se realizará un análisis de los aspectos que se deberán considerar para cumplir con cada uno de estos principios, deberes y derechos en el tratamiento de datos biométricos.

5.4 Obligaciones en torno a los principios y deberes, y recomendaciones para su cumplimiento

Principio de licitud

Fundamento legal

- Artículos 7, primer párrafo, y 9, segundo párrafo, de la LFPDPPP y 10 y 56 de su Reglamento.
- Artículo 7 y 17 de la LGPDPPSO y 8 de los Lineamientos Generales.

¿En qué consiste este principio?

De conformidad con este principio, los datos personales deberán tratarse con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.

En el caso de los sujetos obligados, de manera adicional, el tratamiento de los datos personales que éstos realicen deberá sujetarse a las facultades o atribuciones que la normativa aplicable les confiera.

¿Cuáles son las obligaciones generales que derivan del principio de licitud?

1. Tratar los datos personales de acuerdo con la normatividad que regula el derecho a la protección de datos personales.

[17] El derecho de revocación del consentimiento se encuentra contemplado en la LFPDPPP y en los Lineamientos Generales del sector público, mientras que la prerrogativa de portabilidad está prevista sólo en la LGPDPPSO.

2. Conocer la normatividad que en lo específico regula y aplica a la actividad en la que son tratados los datos personales y realizar el tratamiento en plena observancia de la misma.
3. En el sector público, los sujetos obligados deberán tratar los datos personales que posean de conformidad con las facultades o atribuciones que la normatividad les otorgue.

Asimismo, cuando se trate de datos personales sensibles:

- Los responsables del sector privado no podrán crear bases de datos que contengan datos personales sensibles, sin que se justifique su creación para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el responsable, por disposición legal o para el ejercicio de derechos de terceros.
- Los responsables del sector público no podrán tratar datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos de excepción establecidos en el artículo 22 de la LGPDPPSO.

Recomendaciones específicas para el principio de licitud en el tratamiento de datos biométricos

- Conocer la normatividad que en lo específico regula y aplica a la actividad en la que son tratados los datos biométricos, a fin de verificar que la misma prevea el uso de este tipo de datos y en qué términos lo hace, o bien, que la misma no lo prohíba.
- Revisar las atribuciones que facultan al sujeto obligado para tratar datos biométricos, o bien, en el caso de los responsables del sector privado, analizar si el uso de los datos biométricos está debidamente justificado según la finalidad de la que se trate.

Principio de lealtad

Fundamento legal

- Artículos 7 de la LFPDPPP y 44 de su Reglamento.
- Artículo 19 de la LGPDPPSO y 11 de los Lineamientos Generales.

¿En qué consiste este principio?

Establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, es decir, la confianza que deposita el titular en el responsable, respecto de que los datos personales proporcionados serán tratados conforme a lo que acordaron, así como a lo señalado por la normatividad y el aviso de privacidad correspondiente.

De igual forma establece que el responsable no deberá obtener ni tratar datos personales a través de medios engañosos o fraudulentos.

¿Cuáles son las obligaciones generales que derivan del principio de lealtad?

1. No utilizar medios engañosos o fraudulentos para recabar ni tratar datos personales. Se entiende que existe una acción fraudulenta o engañosa cuando:

- Existe dolo, mala fe o negligencia de la información proporcionada al titular sobre el tratamiento, y
- Las finalidades no se informen en el aviso de privacidad o no sean las que se informen en él.

2. Respetar la expectativa razonable de privacidad del titular.

Recomendaciones específicas para el principio de lealtad en el tratamiento de datos biométricos

- Utilizar medios que estén permitidos por la ley para obtener los datos biométricos.
- Verificar que en el aviso de privacidad se señale de manera expresa el tratamiento de los datos biométricos y que esté incluida la finalidad para la cual se utilizarán.
- Tener especial cuidado en el tratamiento de datos biométrico, a fin de que éste se apegue a lo informado al titular y se privilegie en todo momento sus intereses con relación al uso de sus datos personales.

Principio de información

Fundamento legal

- Artículos 15 al 18 de la LFPDPPP y del 23 al 35 de su Reglamento, Lineamientos y Criterios.
- Artículos 26 al 28 de la LGPDPPSO y del 26 al 45 de los Lineamientos Generales.

¿En qué consiste este principio?

Es el principio en virtud del cual el responsable se encuentra obligado a comunicar al titular de los datos personales las características principales del tratamiento al que será sometida su información personal, así como los medios para ejercer sus derechos, lo que se materializa a través del aviso de privacidad.

En ese sentido, todo responsable que trate datos personales, sin importar la actividad que realice o si se trata de una persona física o moral, pública o privada, requiere elaborar y poner a disposición de los titulares el aviso de privacidad.

Es así que el principio de información legitima el tratamiento de los datos personales, mediante la elaboración y puesta a disposición del aviso de privacidad, entendido éste como el documento físico, electrónico o en cualquier otro formato generado por el responsable, que es puesto a disposición del titular previo al tratamiento de sus datos personales, con el propósito de informarle en qué consistirá el mismo, así como los medios disponibles para ejercer sus derechos.

El aviso de privacidad permite que el titular esté debidamente informado, de forma tal que pueda ejercer su derecho a la autodeterminación informativa y protección de datos personales.

¿Cuáles son las obligaciones generales que derivan del principio de información?

1. Elaborar y poner a disposición de los titulares el aviso de privacidad en los términos que fijen la LGPDPPSO y los Lineamientos Generales en el caso de los sujetos obligados, y la LFPDPPP, su Reglamento y los Lineamientos del Aviso de Privacidad, en el caso de los responsables del sector

privado, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales.

2. Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales o en el momento que indique la normatividad aplicable.
3. Redactar el aviso de privacidad con todos los elementos informativos que señala la norma.
4. Utilizar la modalidad de aviso de privacidad que resulte pertinente.
5. Redactar el aviso de privacidad de forma sencilla, con la información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que faciliten su entendimiento.
6. Generar evidencia para demostrar el cumplimiento del principio de información.

Los responsables a los que les aplique la LFPDPPP pueden consultar los Lineamientos del Aviso de Privacidad y el ABC del aviso de privacidad.

Los responsables a los que les aplique la LGPDPPSO deberán redactar el aviso de privacidad en las modalidades y con los elementos informativos que se señalan en los artículos 27 y 28 de dicho ordenamiento, así como en los Lineamientos Generales.

Para la elaboración y puesta a disposición del aviso de privacidad, el INAI ha desarrollado instrumentos que se encuentran a disposición de los responsables, a los que los remitimos y sugerimos tomar en consideración para el cumplimiento del principio de información, entre ellos:

Herramientas elaboradas por el INAI para facilitar el cumplimiento del principio de información

Para responsables a los que les aplica la LFPDPPP:

1) El Generador de Avisos de Privacidad (http://generador-avisos-privacidad.ifai.org.mx/users/login).
2) La guía El ABC del Aviso de Privacidad (http://abcavisosprivacidad.ifai.org.mx/).
3) El formato de auto-evaluación de aviso de privacidad para responsables (http://inicio.ifai.org.mx/RepositorioGuias/Checklist%20aviso%20de%20privacidad_autoevaluaci%C3%B3n%20responsable%20agosto2016.docx).
4) Modelo de aviso de privacidad corto para video vigilancia (http://inicio.ifai.org.mx/ModelosDeAvisosDePrivacidad/Modelo%20de%20aviso%20de%20privacid ad%20corto%20para%20V-V.pdf).
5) Modelo de aviso de privacidad simplificado en video (http://inicio.ifai.org.mx/ModelosDeAvisosDePrivacidad/videoavisoprivacidad.wmv).
6) La guía para instrumentar medidas compensatorias (http://inicio.inai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensa torias.pdf).

Para los sujetos obligados a los que les aplica la LGPDPPSO:

1) Formato de Autoevaluación de Aviso de Privacidad Sector Público (http://inicio.ifai.org.mx/SitePages/Guia-para-el-Aviso-de-Privacidad.aspx)

Recomendaciones específicas para el principio de información en el tratamiento de datos biométricos

- Informar expresamente en el aviso de privacidad que se recabarán datos biométricos, especificando su tipo (por ejemplo, huellas dactilares o iris).
- Cuando los datos biométricos que se traten sean sensibles, señalarlo en el aviso de privacidad.
- Incluir en el aviso de privacidad las finalidades para las cuales serán tratados los datos biométricos, entre ellas el reconocimiento de los titulares, y en caso de que éstas requieran el consentimiento, señalarlo.
- Cuando se realicen transferencias de datos biométricos, informarlo en el aviso de privacidad y, en caso de que éstas requieran consentimiento, señalarlo.
- Si las finalidades o transferencias de datos biométricos requieren consentimiento, se deberá ofrecer al titular un mecanismo para que pueda otorgar o negar su consentimiento.
- En el caso del sector público, incluir en el aviso de privacidad las disposiciones normativas que fundamentan el tratamiento de los datos biométricos.
- Tomar en cuenta que, debido a la naturaleza de los sistemas biométricos tratados para fines de reconocimiento, normalmente se llevarán a cabo dos etapas en las que estos datos serán recolectados: la primera, para la creación de las plantillas que serán almacenadas en el sistema biométrico; la segunda, para la comparación de nuevas muestras biométricas con las plantillas almacenadas. Al respecto, no es necesario que el responsable dé a conocer el aviso de privacidad integral en cada ocasión que un dato biométrico es recolectado para realizar la comparación si el aviso de privacidad fue dado a conocer con anterioridad a la recolección inicial de un sistema biométrico en particular. No obstante, se recomienda que en cada recolección de datos biométricos, se ponga a disposición del titular el aviso de privacidad simplificado.

Principio de consentimiento

Fundamento legal

- Artículos 8 al 10 de la LFPDPPP y del 11 al 21 de su Reglamento.
- Artículos 7, 20 al 22 de la LGPDPPSO y artículos 12 al 20 de los Lineamientos Generales.

¿En qué consiste este principio?

Como regla general, el responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales, salvo en los casos de excepción previstos en los artículos 10 y 37 de la LFPDPPP, o en el artículo 22 de la LGPDPPSO, según resulte aplicable.

Cuando éste se requiera, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informe en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general. Asimismo, el consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad.

Ahora bien, el consentimiento puede ser tácito, expreso o expreso y por escrito, dependiendo del tipo de datos personales que se tratarán, como se explica a continuación:

Tipo de consentimiento	¿Para qué tipo de datos personales se requiere?		¿Cómo se obtiene?
	LFPDPPP	LGPDPPSO	
Tácito	Para cualquier tipo de dato personal, con excepción de los datos patrimoniales, financieros y sensibles.	Para cualquier tipo de dato personal, con excepción de los datos sensibles.	El consentimiento tácito se obtiene si el titular no se niega a que sus datos personales sean tratados, después de haber conocido el aviso de privacidad. Es decir, no es necesario que quede registrado que el titular autorizó el tratamiento de su información personal, sino que es suficiente con que no se niegue al tratamiento. No obstante, se sugiere que el responsable deje constancia con la que acredite que en su momento puso a disposición del titular el aviso de privacidad.
Expreso	Para datos financieros y patrimoniales.	No se especifica.	El titular deberá expresamente señalar que consiente el tratamiento de sus datos personales. La voluntad del titular se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología.
Expreso-por escrito	Para datos personales sensibles.		El consentimiento se deberá otorgar por escrito, mediante firma autógrafa, huella dactilar, firma electrónica del titular o cualquier otro mecanismo autorizado que permita identificarlo plenamente.

El responsable puede utilizar los siguientes medios para obtener el consentimiento expreso o expreso y por escrito:

El consentimiento expreso o expreso y por escrito se puede obtener a través del aviso de privacidad o de cualquier otro documento físico o electrónico que determine el responsable. Por ejemplo, el consentimiento expreso y por escrito se podría obtener a través de un formato o contrato, y el expreso por medio de una grabación telefónica o de una casilla en formato electrónico. No obstante, hay que recordar que, en todos los casos, de manera previa se debe dar a conocer el aviso de privacidad. Es importante tener en cuenta, que el medio que el responsable ponga a disposición del titular para obtener su consentimiento debe ser sencillo y gratuito.

Adicionalmente, la obtención del consentimiento deberá reunir las siguientes características:

Libre

- Que no medie error, mala fe, violencia o dolo que puedan afectar la manifestación de la voluntad del titular.

Específico

- Que refiera a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales.

Informado

- Que el titular tenga el conocimiento del aviso de privacidad previo al tratamiento al que serán sometidos sus datos personales y que conozca las consecuencias de otorgar su consentimiento.

Inequívoco (sólo para la LFPDPPP)

- Que existan elementos que de manera indubitable demuestren su otorgamiento, en el caso del consentimiento expreso y expreso-por escrito.

La LFPDPPP establece excepciones a la obligación general de obtener el consentimiento para el tratamiento de los datos personales, las cuales se encuentran previstas en el artículo 10 de dicha norma. En particular, no será necesario el consentimiento de los titulares cuando:

- El tratamiento sea necesario porque así lo ordena una ley;
- Los datos personales se obtengan de una fuente de acceso público;
- Los datos personales se sometan a un procedimiento previo de disociación, de forma tal que no se pueda identificar a su titular;
- El tratamiento tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- Los datos personales sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables, y cuando el tratamiento se realice por una persona sujeta al secreto profesional u obligación equivalente, o
- Se dicte resolución de autoridad competente.

Por su parte, el artículo 22 de la LGPDPPSO, establece las excepciones en las que el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales:

- Cuando una ley así lo disponga, sin que dichos supuestos contravengan las bases, principios y disposiciones de la LGPDPPSO;
- Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
- Cuando los datos personales figuren en fuentes de acceso público;
- Cuando los datos personales se sometan a un procedimiento previo de disociación, o
- Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Por último, resulta conveniente señalar que el hecho de que no se requiera el consentimiento para el tratamiento, no implica que no se deban cumplir los otros principios, lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.

¿Cuáles son las obligaciones generales que derivan del principio de consentimiento?

1. Recabar el consentimiento para el tratamiento de datos personales, cuando éste se requiera. Para ello, se deberá identificar, primero, si se actualiza alguna de las causales previstas en el artículo 10 de la LFPDPPP o 22 de la LGPDPPSO y, en caso de que no sea así, se deberá identificar el tipo de datos personales que se van a tratar, para determinar si se requiere el consentimiento tácito, expreso o expreso-por escrito.
2. Solicitar el consentimiento expreso para los datos personales financieros o patrimoniales.
3. Solicitar el consentimiento expreso-por escrito para los datos personales sensibles.
4. Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento.
5. Solicitar el consentimiento siempre ligado a finalidades específicas e informadas en el aviso de privacidad.
6. Solicitar el consentimiento previo a la obtención de los datos personales o en el momento en que lo indique la normatividad que resulte aplicable.
7. Obtener el consentimiento para nuevas finalidades, cuando se pretenda tratar los datos personales para fines distintos, que no sean compatibles o análogos a los establecidos de origen en el aviso de privacidad.
8. Facilitar al titular medios sencillos y gratuitos para que, en su caso, pueda manifestar su consentimiento o negativa al mismo.
9. Generar pruebas para acreditar que se cumplió con el principio de consentimiento.
10. Llevar un control para identificar a los titulares que en su caso hayan negado su consentimiento para el tratamiento de finalidades específicas, que no se traten de aquéllas que originan y sustentan la relación jurídica entre el titular y el responsable.

Para conocer algunas recomendaciones adicionales sobre cómo cumplir con el principio de consentimiento, se sugiere consultar la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en el portal del INAI (www.inai.org.mx) o en la dirección electrónica:
http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Recomendaciones específicas para el principio de consentimiento en el tratamiento de datos biométricos.

- Primeramente, se sugiere identificar si el dato biométrico recolectado será tratado dentro de alguno de los supuestos previstos por los artículos 10 de la LFPDPPP o 22 de la LGPDPPSO. En caso de que así sea, su tratamiento no requerirá consentimiento.
- No obstante, si el responsable pretende utilizar los datos biométricos para finalidades que no encuadren en las excepciones anteriormente señaladas, o que no resulten compatibles o análogas con aquéllas para las cuales se recabaron los datos personales, será necesario que se obtenga el consentimiento del titular.

- Solicitar el consentimiento tácito de los titulares de los datos biométricos, cuando éstos no resulten sensibles.
- Solicitar el consentimiento expreso y por escrito de los titulares de los datos biométricos, previo a que se recaben, o bien, en el momento en que lo indique la normativa aplicable, cuando éstos resulten sensibles.

NOTA: Lo relacionado con el consentimiento requerido para realizar transferencias de datos biométricos y sus excepciones será desarrollado en el apartado correspondiente al régimen de transferencias.

Principio de finalidad

Fundamento legal

- Artículos 4, 9, segundo párrafo, 10 y 12 de la LFPDPPP y del 40 al 43 y 56 de su Reglamento.
- Artículo 18 de la LGPDPPSO y artículos 9 y 10 de los Lineamientos Generales.

¿En qué consiste este principio?

En atención a este principio, los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste, o bien, para aquellas finalidades que sean compatibles o análogas.

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales. Las finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

De igual forma, los sujetos obligados de la LGPDPPSO deberán realizar los tratamientos que estén justificados por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera. Estos responsables podrán tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre que cuenten con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que el titular sea una persona reportada como desaparecida, en los términos previstos en la LGPDPPSO y demás disposiciones que resulten aplicables en la materia.

Por último, es importante recordar que en el caso de que los datos biométricos sean también datos personales sensibles, los responsables del sector privado no podrán crear bases de estos datos sin que se justifique su creación para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el responsable u obedezca a un mandato legal.

¿Cuáles son las obligaciones generales que derivan del principio de finalidad?

- Tratar los datos personales sólo para el cumplimiento de la finalidad o finalidades que se informaron en el aviso de privacidad, o aquéllas que resulten compatibles o análogas.
- No condicionar que para el tratamiento de los datos personales para las finalidades necesarias o que dan origen a la relación jurídica entre el responsable y el titular, se requiera el tratamiento de datos personales para finalidades que no son necesarias o no dan origen a la relación jurídica.

- No tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiesen recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, a menos que lo permita una ley o reglamento o se obtenga el consentimiento del titular de los datos.
- En el caso de sujetos obligados del sector público, no tratar los datos personales para finalidades distintas de aquéllas para las que se hubiesen recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, a menos que éstos cuenten con atribuciones conferidas en la normativa y medie el consentimiento del titular, salvo que los datos personales pertenezcan a una persona reportada como desaparecida.

Recomendaciones específicas para el principio de finalidad en el tratamiento de datos biométricos

- Describir en el aviso de privacidad la o las finalidades para las cuales serán tratados los datos biométricos recolectados. En el caso de que los datos biométricos se utilicen para el reconocimiento de personas, incluirlo en el aviso de privacidad como una finalidad más.
- No tratar los datos biométricos del titular para finalidades distintas, que no resulten compatibles o análogas a aquéllas para las cuales fueron recabados, por ejemplo, para conocer su estado de salud en el caso de que se hayan recabado para el control de acceso a instalaciones.
- Cuando los datos biométricos que se recaben se consideren sensibles, las finalidades para las cuales se recaben y traten los datos biométricos deberán estar debidamente justificadas. Para el caso de los particulares, estas finalidades deberán ser legítimas, concretas y acordes con las actividades del responsable. Por su parte, para el caso del sector público, las finalidades deberán estar debidamente fundamentadas, además de motivadas.

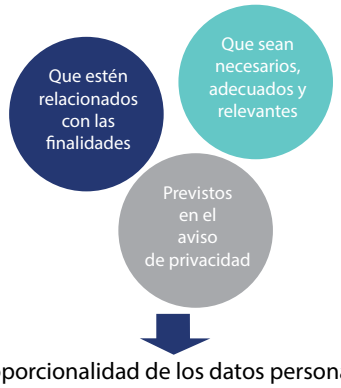
Principio de proporcionalidad

Fundamento legal

- Artículos 13 de la LFPDPPP y 45 y 46 de su Reglamento.
- Artículo 25 de la LGPDPPSO y artículos 24 y 25 de los Lineamientos Generales.

¿En qué consiste este principio?

En atención a este principio sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido y que se encuentren previstas en el aviso de privacidad.



De igual forma, el responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron.

Con relación al tratamiento de datos personales sensibles, los responsables deberán realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable, con relación a las finalidades que motivan su tratamiento.

¿Cuáles son las obligaciones generales que derivan del principio de proporcionalidad?

- Realizar esfuerzos razonables para que los datos personales que se recaben, sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.
- Tratar sólo los datos personales necesarios, adecuados y relevantes para la finalidad que se obtuvieron.
- Limitar el periodo de tratamiento de los datos personales al mínimo indispensable, especialmente si son sensibles.

Recomendaciones específicas para el principio de proporcionalidad en el tratamiento de datos biométricos.

- Evaluar si la recolección de datos biométricos es necesaria para la finalidad pretendida.
- Priorizar el uso de datos que no sean biométricos para lograr la misma finalidad sin restarle efectividad.
- Obtener y utilizar únicamente los datos biométricos que sean necesarios, adecuados y no excesivos para las finalidades para las que fueron recabados. Por ejemplo, se recomienda adquirir sistemas biométricos en donde se eliminen las muestras biométricas inicialmente recolectadas y se almacenen únicamente las plantillas obtenidas de dichas muestras y que son las que se utilizarán para futuras comparaciones.
- Recolectar y tratar el número mínimo de datos biométricos (muestras biométricas) necesarios para la finalidad para la cual se están recolectando. Por ejemplo, para los procesos de control de acceso, es recomendable priorizar sistemas biométricos de verificación sobre los de identificación.
- Evitar o limitar al máximo la recolección de datos biométricos que pudieran revelar datos sensibles no necesarios para las finalidades legítimas que se persiguen. Por ejemplo, la muestra del iris usada para control de acceso podría revelar información sobre el estado de salud de la persona, la cual es excesiva para dicha finalidad.
- La cantidad de muestras biométricas también depende de su calidad, es decir, entre más precisas y exactas sean las muestras biométricas y las plantillas recolectadas y generadas, será necesario recolectar un menor número de muestras biométricas por individuo. Por ello, es recomendable recabar datos con la mejor calidad posible para disminuir el número de datos biométricos requeridos para cumplir con la finalidad correspondiente. En este sentido, de acuerdo con el análisis de los sistemas biométricos para reconocimiento dactilar realizado por NIST,[18] la utilización de cuatro a diez huellas dactilares resulta tan eficiente como la utilización de una sola huella dactilar de alta calidad. Sólo en ciertos casos, por ejemplo, cuando una autoridad realice un tratamiento de huellas dactilares con una finalidad vinculada con un tema de seguridad nacional o pública, podría justificarse la recolección de un mayor número de datos.

[18] Instituto Nacional de Estándares de los Estados Unidos de América (NIST, por sus siglas en inglés).

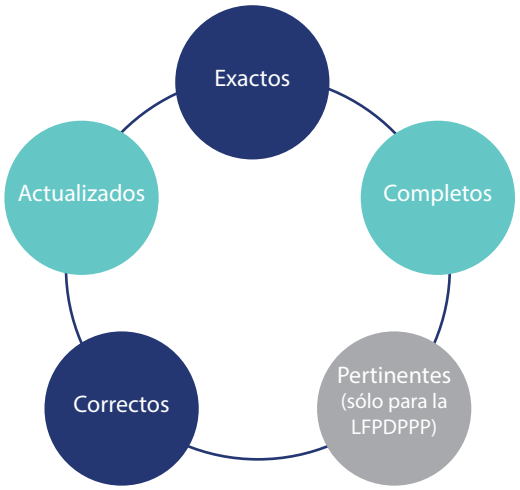
Principio de calidad

Fundamento legal

- Artículos 11 de la LFPDPPP y del 36 al 39 de su Reglamento.
- Artículos 23 y 24 de la LGPDPPSO y artículos 21 a 23 de los Lineamientos Generales.

¿En qué consiste este principio?

El principio de calidad significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos sean:



- Los datos personales son **exactos** cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.
- Los datos personales están **completos** cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular.
- Los datos personales son **pertinentes** cuando corresponden efectivamente al titular y que se relacionan y son adecuados para realizar la finalidad para la cual fueron recabados.
- Los datos están **actualizados** cuando están al día y corresponden a la situación presente del titular.
- Los datos personales son **correctos** cuando no tienen errores o defectos y en ese sentido cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

El responsable debe adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con estas características, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

Asimismo, este principio establece la obligación del responsable de suprimir o eliminar previo bloqueo –en caso de que fuera requerido- los datos personales que hayan dejado de ser necesarios para el cumplimiento de las finalidades que originaron su tratamiento, salvo que por disposiciones legales y por consideraciones administrativas, contables, fiscales, jurídicas o históricas, deban ser conservados por más tiempo.

Se presume que se cumple con la calidad de los datos, cuando éstos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que lo contradiga.

¿Cuáles son las obligaciones generales que derivan del principio de calidad?

1. Adoptar los mecanismos necesarios para procurar que los datos personales en posesión del responsable sean exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que el titular se vea afectado por dicha situación.
2. Conservar los datos personales exclusivamente hasta en tanto la finalidad para la cual se recabaron haya sido satisfecha y por el tiempo establecido en las disposiciones legales aplicables, tomando en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
3. Bloquear los datos personales una vez que concluya el plazo de conservación, para limitar su uso exclusivamente, y sólo en caso de que sea necesario, para determinar responsabilidades en relación con su tratamiento.
4. Suprimir los datos personales una vez terminado el periodo de bloqueo, siempre que no exista una disposición legal que obligue a la conservación de la información o que la misma tenga valor histórico.
5. Los responsables a quienes les aplica la LFPDPPP deberán eliminar los datos personales relacionados al incumplimiento de obligaciones contractuales, previo bloqueo, una vez que transcurra un plazo de 72 meses, contado a partir de la fecha en que se presente el incumplimiento.
6. Tomar medidas razonables para que se cumpla el principio de calidad, teniendo en cuenta siempre el tipo de datos personales y las condiciones de tratamiento, cuando los datos personales no se obtengan directamente del titular.
7. Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales, que incluyan los periodos de conservación.
8. Contar con un procedimiento o mecanismo que le permita demostrar que los datos personales se conservan, bloquean, suprimen o cancelan cumpliendo los plazos establecidos para ello, o en atención a una solicitud del derecho de cancelación.

Recomendaciones específicas para el principio de calidad en el tratamiento de datos biométricos

- Los responsables deberán tomar todas las medidas razonables para garantizar que los datos biométricos en su poder sean exactos, completos, pertinentes y actualizados.
- Es importante señalar que la exactitud[19] de las plantillas y la calidad de las muestras biométricas depende de diversos factores como:
  - La tecnología o el sistema biométrico utilizado. Al respecto, es recomendable utilizar tecnología o sistemas biométricos que garanticen la mayor calidad posible en la obtención de las muestras biométricas y que tengan tasas bajas de falsos positivos y de falsos negativos.[20] No obstante,

[19] Que tengan contraste y resolución, sean comprimidas correctamente y no presenten distorsiones.

[20] Se considera oportuno recordar nuevamente que las tasas de falsos positivos y falsos negativos son variables dependientes y cuando una sube, la otra baja, por lo que la decisión para establecer el umbral de coincidencia debe ser analizado a fondo.

es importante reconocer que, hasta el momento, no hay tecnología o sistema biométrico que garantice un 100 por ciento de exactitud.[21]

- Si se lleva a cabo un proceso de verificación o de identificación. La calidad de las muestras biométricas y la exactitud de las plantillas requerida para procesos de identificación es mayor que la requerida en procesos de verificación.
- La naturaleza del propio biométrico, ya que hay algunos más estables que otros y que facilitan comparaciones útiles para efectos de reconocimiento. El iris y la huella dactilar tienden a tener menos variaciones que la voz o la imagen facial, que pueden distorsionarse por el entorno de captura y tienen características no lineales (la misma persona puede tener distintos tonos de voz o expresiones faciales).
- El tamaño de la base de datos biométricos a compararse. Entre mayor sea el número de datos biométricos a compararse, se requerirá una mayor calidad en la muestra biométrica recolectada y en la exactitud de la plantilla generada.

- No conservar los datos biométricos por un plazo superior al necesario para cumplir con la finalidad para la que se han recolectado. Por ejemplo, si los datos biométricos de un empleado han sido recolectados para controlar el acceso a las instalaciones o sistemas informáticos del empleador, dichos datos deberían eliminarse tan pronto como concluya el plazo en el que se puedan utilizar para un procedimiento jurídico o administrativo, o bien, se termine la relación laboral.

Principio de responsabilidad

Fundamento legal

- Artículo 14 de la LFPDPPP y 47 y 48 de su Reglamento.
- Artículos 29 y 30 de la LGPDPPSO y artículos 46 a 52 de los Lineamientos Generales.

¿En qué consiste este principio?

El responsable deberá velar por el cumplimiento de los principios de protección de datos personales, con relación a los datos que se encuentren bajo su custodia o posesión o aquéllos que haya comunicado a un encargado, así como rendir cuentas de su tratamiento.

Para cumplir con este principio, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación vinculante o cualquier otro mecanismo que determine adecuado para tales fines, siempre observando las disposiciones de la Constitución Política de los Estados Unidos Mexicanos y los Tratados Internacionales en los que el Estado mexicano sea parte.

¿Cuáles son las obligaciones generales que derivan del principio de responsabilidad?

- Velar por el cumplimiento de los principios, deberes y obligaciones establecidos en las leyes de protección de datos personales, debiendo adoptar las medidas necesarias para su aplicación e

[21] Según Aware, Inc., los sensores de los sistemas biométricos producen distorsiones ópticas y eléctricas, sobre la muestra biométrica. Asimismo, en el momento de la conversión a plantilla biométrica hay información de la muestra biométrica que se pierde. En el mismo sentido, señala que "[l]as frecuencias de muestreo (resolución espacial en el dominio digital) tienen un impacto significativo sobre la calidad de muestras biométricas", entre otros aspectos a considerarse.

implementar los mecanismos para acreditar su cumplimiento. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable.

- Adoptar, al menos los siguientes mecanismos o medidas para cumplir con el principio de responsabilidad:
  - Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable. Para ello, se sugiere consultar el material que ha desarrollado el INAI para conocer bien las obligaciones que tiene todo responsable en el tratamiento de datos personales;
  - Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales. Al respecto, sugerimos visitar nuestro campus virtual CEVINAI, disponible en http://cevifaiprivada.ifai.org.mx/swf/cevinaiv2/cevinai/index.php y otros cursos impartidos por el INAI;
  - Destinar recursos para la instrumentación de los programas y políticas de privacidad. En el caso de los sujetos obligados de la LGPDPPSO, dichos recursos deberán estar autorizados;
  - Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
  - Establecer procedimientos para recibir y responder dudas y quejas de los titulares, y
  - Prever un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

Además de las obligaciones anteriores, los responsables a quienes les aplica la LFPDPPP deberán:

- Velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano. Para cumplir lo anterior, podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines;
- Tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento al interior de su organización o por terceros con los que guarde alguna relación jurídica;
- Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;
- Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones establecidas por la LFPDPPSP;
- Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento, y
- Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.

Por su parte, los responsables a quienes les aplica la LGPDPPSO, deberán:

- Rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto o a los Organismos garantes, según corresponda, caso en el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines;
- Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia, y
- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.

Cabe señalar que los mecanismos necesarios para dar cumplimiento al principio de responsabilidad por parte de los sujetos obligados del sector público, se encuentran desarrollados a mayor detalle en los Lineamientos Generales.

Recomendaciones específicas para el principio de responsabilidad en el tratamiento de datos biométricos

- Instrumentar procedimientos para que se evalúe y atienda el riesgo por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios que impliquen el tratamiento de datos biométricos; así como para mitigar los riesgos identificados.
- Implementar Privacidad por Diseño (es decir, tomar en cuenta los principios rectores de la protección de datos personales desde la fase inicial de diseño de cualquier desarrollo tecnológico) y, en su caso, Evaluaciones de Impacto a la Protección de Datos Personales.
- Vigilar y documentar el desempeño del personal y prever acciones disciplinarias apropiadas y proporcionales -cuando la normativa laboral aplicable así lo permita- para aquellos empleados que no cumplan debidamente sus deberes en el manejo de datos personales, incluidos los datos biométricos.
- Asegurarse que los servicios prestados por cualquier encargado que realice tratamiento de datos personales –incluidos los datos biométricos- a nombre y por cuenta del responsable se apegue a los artículos 50 a 55 del Reglamento de la LFPDPPP, en caso de particulares, o bien, a los artículos 58 al 64 de la LGPDPPSO, en el caso de Sujetos Obligados, los cuales se desarrollan en el apartado de las obligaciones derivadas de la relación con encargados del tratamiento de esta guía.
- Supervisar constantemente las actividades realizadas por proveedores externos que ofrezcan servicios que involucren el tratamiento de datos biométricos.
- Adoptar esquemas de autorregulación vinculante o buenas prácticas en el tratamiento de datos biométricos.

Deber de seguridad

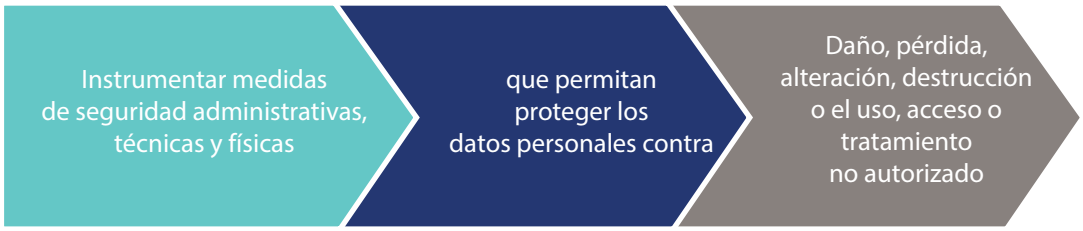
Fundamento legal

- Artículos 19 y 20 de la LFPDPPP y Capítulo III de su Reglamento.
- Artículos 31 al 41 de la LGPDPPSO y artículos 55 a 70 de los Lineamientos Generales.

¿En qué consiste?

Un pilar básico para un efectivo sistema de protección de datos personales es la seguridad de los datos personales, entendida como la implementación de medidas administrativas, físicas y técnicas para garantizar y velar por la integridad, confidencialidad y disponibilidad de los datos personales.

Por lo tanto, todo responsable y encargado que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.



De conformidad con la LFPDPPP, el responsable no podrá adoptar medidas para la seguridad de los datos personales, menores a aquéllas que tenga implementadas para la protección de su información en general.

Asimismo, tanto la LFPDPPP como la LGPDPPSO prevén que, para el establecimiento de las medidas o controles de seguridad, se deberá tomar en cuenta:

- El riesgo inherente a los datos personales tratados;
- Las posibles consecuencias de una vulneración;
- La sensibilidad de los datos personales;
- El desarrollo tecnológico;
- El número de titulares;
- Las vulneraciones previas ocurridas en los sistemas de tratamiento;
- El riesgo por el valor potencial cualitativo o cuantitativo que pudieran tener los datos personales para una persona no autorizada para su posesión, y
- Demás factores que puedan incidir en el nivel de riesgo –como las transferencias de datos personales que se realicen- o que resulten de otras leyes o regulación aplicable al responsable.

Asimismo, el responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos. Para ello, el responsable deberá informar al titular al menos lo siguiente:

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

Además de lo anterior, en caso de que ocurra una vulneración a los datos personales, el responsable debe analizar las causas por las cuales se presentó y a efecto de evitar que la vulneración se repita, deberá implementar acciones correctivas, preventivas y de mejora.

En el caso del sector público, el responsable que sufra una vulneración deberá informar también al INAI o al organismo garante que corresponda. Los Lineamientos Generales desarrollan con mayor detalle aspectos sobre plazos y los requerimientos de esta notificación.

Otra obligación adicional que tienen los responsables del sector público, es la elaboración de un documento de seguridad con la siguiente información:

- El inventario de datos personales y de los sistemas de tratamiento;
- Las funciones y obligaciones de las personas que traten datos personales;
- El análisis de riesgos;
- El análisis de brecha;
- El plan de trabajo;
- Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- El programa general de capacitación.

El documento de seguridad deberá actualizarse en los siguientes casos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

¿Cuáles son las obligaciones generales que derivan del deber de seguridad?

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas necesarias para el manejo de los datos personales en general.
2. Tomar en cuenta el riesgo inherente por tipo de dato personal; las posibles consecuencias para los titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento, 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, entre otros factores que pudieran influir en el nivel de riesgo.
3. Considerar las acciones que establece el artículo 61 del Reglamento de la LFPDPPP o 33 de la LGPDPDPSO para la implementación y mantenimiento de las medidas de seguridad. Para ello, se recomienda consultar los documentos de apoyo que se enlistan más adelante.
4. Actualizar las medidas de seguridad implementadas –y el documento de seguridad, cuando así se requiera-, según los criterios antes descritos.
5. Notificar a los titulares, y en su caso al INAI, las vulneraciones de seguridad que se presenten cuando éstas afecten de forma significativa sus derechos patrimoniales o morales.
6. Llevar a cabo las acciones que sean necesarias para corregir o prevenir que la vulneración de seguridad se repita.

Por su parte, los sujetos obligados de la LGPDPPSO además deberán:

1. Contar con un sistema de gestión que documente las acciones relacionadas con las medidas de seguridad previstas en el artículo 33 de la LGPDPPSO,
2. Elaborar un documento de seguridad[22] y actualizarlo, y
3. Llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Es importante que los sujetos obligados de la Ley General observen cómo cumplir con las obligaciones de este deber y el establecimiento de las medidas correspondientes, de conformidad con las especificaciones previstas en los Lineamientos Generales.

Por otro lado, cabe señalar que el INAI publicó las Recomendaciones en materia de seguridad de datos personales en el DOF el 30 de octubre de 2013. Estas recomendaciones sirven de orientación tanto a los responsables como a los encargados del sector privado, para determinar qué procedimientos y mecanismos deben aplicar para garantizar la seguridad de los datos personales.

Además, el INAI desarrolló la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales y una metodología de análisis de riesgo, ambas publicadas en septiembre de 2013, en el portal de Internet del Instituto (**www.inai.org.mx**), así como el Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas, publicado en dicho portal en julio de 2014.

[22] El documento de seguridad debe estar integrado por: i) el inventario de datos personales y de los sistemas de tratamiento; ii) las funciones y obligaciones de las personas que traten datos personales; iii) el análisis de riesgos; iv) el análisis de brecha; v) el plan de trabajo; vi) los mecanismos de monitoreo y revisión de las medidas de seguridad, y vii) el programa general de capacitación. El contenido de cada uno de éstos, se encuentra descrito en los Lineamientos Generales.

Por la especificidad y el nivel técnico del tema, para cumplir con el deber de seguridad, se sugiere consultar las herramientas citadas a continuación, todas ellas disponibles en las direcciones electrónicas especificadas, o bien, en el portal del Internet del INAI (www.inai.org.mx), en la sección de "Protección de Datos Personales".

Herramientas elaboradas por el INAI en materia de cumplimiento al deber de seguridad

1) Recomendaciones en materia de seguridad de datos personales (http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%2 0DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf)
2) Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_S GSDP(Junio2015).pdf)
3) Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas (http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf)
4) Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales (http://inicio.ifai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2 015).pdf)

Recomendaciones específicas para el deber de seguridad en el tratamiento de datos biométricos

- Implementar las medidas físicas, técnicas y administrativas necesarias para garantizar que los datos biométricos estén protegidos del acceso, procesamiento, eliminación, pérdida o uso no autorizados. Para decidir el tipo de medidas a implementar, se recomienda tener en cuenta aspectos como la unicidad del biométrico tratado, su estabilidad en el tiempo, la posibilidad o no de usarlo para distintos fines, la posibilidad de ser obtenidos sin el conocimiento ni consentimiento del titular, y el impacto sobre el titular en caso de robo.
- Revisar que la tecnología biométrica contemple mecanismos de cifrado en el almacenamiento y el tránsito de los datos.
- Restringir el acceso a los datos biométricos únicamente a personal autorizado.
- Guardar en bitácoras todos los accesos a los datos biométricos.
- Evitar cruces de información innecesarios entre los sistemas biométricos y otros sistemas de tratamiento.
- Se sugiere adquirir sistemas biométricos que almacenen únicamente la plantilla con minucias de huellas dactilares en lugar de la representación completa de la misma para que sea más difícil su recreación en caso de que la información sea robada.
- Minimizar el uso de bases de datos centralizadas para el almacenamiento de biométricos.
- Contar con un sitio alterno para resguardar las bases de datos biométricos, el cual deberá estar provisto con las medidas de seguridad suficientes.
- Considerar lo previsto por estándares internacionales, por ejemplo, los generados por el grupo de trabajo ISO/IEC JTC 1/SC 27,[23] en donde se desarrollan aspectos de seguridad en tecnologías de la información, incluidos los relacionados con información biométrica.

[23] Véase: https://www.iso.org/committee/45306.html

Deber de confidencialidad

Fundamento legal

- Artículo 21 de la LFPDPPP.
- Artículo 42 de la LGPDPPSO y 71 de los Lineamientos Generales.

¿En qué consiste?

El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de los datos personales, obligación que subsistirá aun después de finalizar su relación con el titular, o en el caso del encargado o de un empleado, con el responsable.

¿Cuáles son las obligaciones generales que derivan del deber de confidencialidad?

1. Guardar secreto respecto de los datos personales que son tratados en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con el titular.
2. Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.
3. Establecer controles o mecanismos que tengan por objeto que todas las personas que intervengan en cualquier fase del tratamiento de datos personales, incluidos los propios empleados del responsable, eviten la divulgación de éstos.

Recomendaciones específicas para el deber de confidencialidad en el tratamiento de datos biométricos

- No difundir datos biométricos a terceros sin consentimiento de su titular.
- Mantener el secreto de la información relacionada con los datos biométricos recabados y almacenados, excepto cuando su comunicación se encuentre permitida en términos de una disposición legal.
- Definir claramente al personal autorizado para tener acceso y para tratar datos biométricos al interior de la organización, o bien, por terceros que actúen a nombre y por cuenta del responsable. Al respecto, se considera pertinente el uso de cláusulas contractuales que delimiten las obligaciones de los empleados dentro de la organización, así como del encargado.
- Implementar las medidas de seguridad necesarias para garantizar la secrecía de los datos biométricos.

5.5 Obligaciones en torno a las transferencias y recomendaciones para su cumplimiento

Fundamento legal

- Artículos 36 y 37 de la LFPDPPP y Capítulo IV del Reglamento
- Título Quinto de la LGPDPPSO y Título Quinto de los Lineamientos Generales.

¿Qué es una transferencia?

Es toda comunicación de datos personales realizada a persona distinta del responsable que posee los datos personales, del encargado o del titular de los datos personales.

Las transferencias pueden ser:

A. Nacionales, realizadas dentro del territorio mexicano.
B. Internacionales, realizadas fuera del territorio nacional y serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales.

Para que un responsable pueda transferir los datos personales, dentro o fuera de México, es necesario que:

1. Se informe al titular en el aviso de privacidad correspondiente lo siguiente: que la transferencia puede ocurrir, a quién se transferirán los datos y para qué fines. Asimismo, dicho aviso deberá contener una cláusula para que el titular acepte o no la transferencia, en caso de que ésta requiera consentimiento;
2. El titular haya otorgado su consentimiento para que la transferencia se realice, salvo los casos de excepción previstos en el artículo 37 de la LFPDPPP o 70 de la LGPDPPSO, y
3. El objeto de la transferencia se deberá limitar a la finalidad y condiciones informadas en el aviso de privacidad, y que hayan sido consentidas por el titular, en su caso. Para ello, el responsable que transfiere comunicará al responsable que recibe los datos personales, el aviso de privacidad correspondiente.

Los responsables del sector privado no requerirán el consentimiento de los titulares para realizar una transferencia de datos personales, en los siguientes casos (artículo 37 de la LFPDPPP):

- Esté prevista en una ley o tratado en los que México sea parte;
- Sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
- Sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
- Sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- Sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
- Sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
- Sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

Los sujetos obligados del sector público no requerirán el consentimiento de los titulares para realizar una transferencia, en los siguientes casos (artículo 70 de la LGPDPPSO):

- Esté prevista en alguna ley, en convenios o Tratados Internacionales suscritos y ratificados por México;
- Cuando se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- Cuando sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- Cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- Cuando sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- Cuando sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;
- Cuando sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la LGPDPPSO, o
- Cuando sea necesaria por razones de seguridad nacional.

Es importante tener en cuenta que la comunicación de los datos personales a un tercero que administre un sistema biométrico que opera por cuenta y nombre del responsable no se considera una transferencia, sino una remisión, por lo que no existe una obligación de informarla en el aviso de privacidad ni de obtener el consentimiento del titular para que ocurra.

En cambio, cuando haya una comunicación entre el responsable y un nuevo responsable para tratamientos sobre los que este segundo responsable tiene poder de decisión, dicha comunicación se considera una transferencia, por lo que es necesario informarla en el aviso de privacidad y cumplir con las obligaciones previstas en esta sección.

¿Cuáles son las obligaciones generales que derivan del régimen de transferencias?
Existe una serie de obligaciones para los responsables y receptores de datos personales que deberán ser cumplidas, a saber:

A. Obligaciones del responsable que transfiere los datos personales:
    - Informar al titular, a través del aviso de privacidad, las transferencias a las que serán sometidos sus datos personales, los receptores y finalidades de las mismas. En el caso de sujetos obligados, éstos deberán informar los elementos señalados de aquellas transferencias que realicen y requieran consentimiento;
    - Limitar las transferencias a lo convenido en el aviso de privacidad;

- Comunicar a los terceros receptores el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento;
- Obtener el consentimiento del titular para las transferencias, salvo en el caso de que aplique algunas de las excepciones previstas en el artículo 37 de la LFPDPPP o en el artículo 70 de la LGPDPPSO;
- En caso de ser necesario el consentimiento, incluir en el aviso de privacidad un mecanismo en el que el titular pueda manifestar si acepta o no la transferencia de sus datos, y
- Probar que la transferencia se realizó conforme a lo que establece la LFPDPPP y su Reglamento, o bien, conforme a la LGPDPPSO.

B. Obligaciones adicionales para responsables del sector privado que transfieren datos personales:

- En las transferencias nacionales, formalizar la transferencia mediante algún instrumento jurídico como un contrato, que permita demostrar que el responsable comunicó al tercero receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales, y
- En las transferencias internacionales, acordar o celebrar con el tercero receptor cláusulas contractuales u otros instrumentos jurídicos, en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

C. Obligaciones adicionales para los responsables que son sujetos obligados de la LGPDPPSO que transfieren datos personales:

- Formalizar la transferencia mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, salvo en los siguientes casos:
  i. Cuando sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, y
  ii. Cuando sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.
- Transferir o hacer remisión de datos personales fuera del territorio nacional, sólo cuando el tercero receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la Ley.
- Cuando lo considere necesario, el responsable podrá solicitar la opinión del Instituto respecto aquellas transferencias internacionales de datos personales que pretenda efectuar, para lo cual deberá cumplir con los requisitos señalados en el artículo 117 de los Lineamientos Generales.

D. Obligaciones del receptor de los datos personales:

- Tratar los datos personales de conformidad con lo convenido en el aviso de privacidad. Es decir, limitar el tratamiento de los datos transferidos a las finalidades que justificaron las transferencias;

- Asumir las mismas obligaciones que corresponden al responsable que transfirió los datos, incluyendo el deber de confidencialidad, y
- En el caso del receptor que reciba datos personales de un responsable del sector privado, deberá probar que la transferencia se realizó conforme a lo que establece la LFPDPPP y su Reglamento.

Recomendaciones específicas para el régimen de transferencias en el tratamiento de datos biométricos

- Identificar las transferencias que se vayan a realizar de datos biométricos, a fin de cumplir en todos los casos con las obligaciones antes descritas.
- Informar a través del aviso de privacidad las transferencias que se realizarán, el tercero receptor y las finalidades.
- No realizar transferencias de datos biométricos a terceros no autorizados por los titulares, salvo que se actualicen las excepciones previstas en el artículo 37 de la LFPDPPP o los artículos 22 y 70 de la LGPDPPSO.
- Solicitar el consentimiento expreso y por escrito para transferir datos biométricos, cuándo éstos sean considerados como sensibles.
- Eliminar vínculos innecesarios entre la base de datos biométricos con otros sistemas informáticos o bases de datos que inadvertidamente puedan dar lugar a una transferencia no autorizada.
- Cifrar los datos biométricos que se transfieran.
- Considerar lo previsto por estándares internacionales, por ejemplo, los generados por el grupo de trabajo ISO/IEC JTC 1/SC 27, en donde se desarrollan aspectos de seguridad en tecnologías de la información, incluidos los relacionados con información biométrica.

5.6 Obligaciones en torno a los encargados del tratamiento y recomendaciones para su cumplimiento

Fundamento legal

- Artículos 3, fracción IX de la LFPDPPP y artículo 2, fracción XV, 49 a 54 de su Reglamento.
- Título Cuarto de la LGPDPPSO y Título Cuarto de los Lineamientos Generales.

¿Quién es el encargado del tratamiento?

Es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que los vincula y delimita su actuación para la prestación de un servicio.

El encargado no decide sobre el tratamiento de los datos personales, sino que los trata por cuenta del responsable, siguiendo sus instrucciones.

Hay que considerar que la relación entre el responsable y el encargado deberá estar establecida mediante contrato, cláusulas u otro instrumento jurídico, que decida el responsable y que permita acreditar su existencia, alcance y contenido.

En todo caso, los acuerdos que se alcancen entre el responsable y el encargado deberán ser acordes con lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales, entre el responsable y el titular.

Tratándose de datos biométricos, se deberá considerar como encargado al tercero que realiza la recolección de muestras, creación de plantillas, almacenamiento de datos biométricos o su comparación, por nombre y cuenta de un responsable quien es el que decide sobre el tratamiento de los datos personales.

Por otra parte, es importante considerar que existen supuestos en los que un encargado será considerado como responsable, con las obligaciones propias de éste. En específico, cuando:

a) Incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales, por ejemplo, destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o

b) Efectúe una transferencia, incumpliendo las instrucciones del responsable.

¿Qué es una remisión?

A diferencia de las trasferencias de datos personales entre un responsable y un tercero, la comunicación de datos personales entre el responsable y el encargado se conoce como remisión, la cual podrá ser dentro o fuera del territorio mexicano.

Las remisiones de datos personales no requerirán ser informadas al titular, ni contar con su consentimiento. No obstante, existen obligaciones vinculadas con las mismas.

¿Cuáles son las obligaciones en la relación responsable-encargado?

El encargado tendrá las siguientes obligaciones respecto del tratamiento de los datos personales que realice por cuenta del responsable:

- Tratar los datos personales únicamente conforme a las instrucciones del responsable.
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
- Implementar las medidas de seguridad conforme a la normativa aplicable.
- Guardar confidencialidad respecto de los datos personales tratados.
- Suprimir (o devolver[24]) los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones de éste, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

[24] En el caso de los datos biométricos, por su propia naturaleza, la devolución podría no resultar viable.

- Solicitar autorización al responsable para subcontratar servicios que impliquen el tratamiento de datos personales, previo a la subcontratación, en caso de que la misma no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos, mediante los cuales se formalizó la relación con el responsable.
- Formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que acredite su existencia, alcance y contenido, una vez obtenida la autorización.

Adicionalmente, los encargados de responsables sujetos obligados a la LGPDPPSO, tienen la obligación de informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones, ya que éstos serán corresponsables por las vulneraciones de seguridad ocurridas en el tratamiento de datos personales que efectúe el encargado a nombre y por cuenta de los responsables.

Por su parte, el responsable tendrá las siguientes obligaciones al momento de establecer una relación con un encargado:

1. Establecer la relación con el encargado a través de un instrumento jurídico que permita acreditar la existencia de la relación jurídica, su contenido y alcance.
2. Fijar los acuerdos con el encargado con base en lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales.
3. Contemplar en el instrumento que establezca la relación jurídica con el encargado, al menos, las obligaciones que prevé el artículo 50 del Reglamento de la LFPDPPP o 59 de la LGPDPPSO.
4. Autorizar, en caso de que así lo desee, las subcontrataciones que realice el encargado, que involucren el tratamiento de datos personales.
5. Verificar que el encargado cumpla con sus obligaciones.
6. Los responsables de la LGPDPPSO deberán, además, prever en el contrato o instrumento jurídico, las siguientes obligaciones para el encargado:
   a. Permitir al Instituto o responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales;
   b. Colaborar con el Instituto en las investigaciones previas y verificaciones, así como
   c. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.
7. Contratar servicios de cómputo en la nube que cumplan, al menos, con las condiciones descritas en el artículo 52 del Reglamento de la LFPDPPP o 64 de la LGPDPPSO, especificados en la siguiente tabla:

Condiciones de contratación de cómputo en la nube
Cumplir con: • Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables a la normativa. • Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; • Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y • Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

Condiciones de contratación de cómputo en la nube
Contar mecanismos para: • Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; • Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; • Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; • Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, e • Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso.

Recomendaciones específicas para la relación responsable-encargado en el tratamiento de datos biométricos

- Establecer una relación con encargados que cuentan con experiencia y buen nombre en el tratamiento de datos biométricos.
- Que la relación entre el responsable y el encargado que recolecte muestras biométricas, elabore plantillas, las almacene o realice las comparaciones, se sustente a través de un instrumento jurídico, en el que se establezcan con claridad los términos, condiciones e instrucciones para el tratamiento de los datos personales, y en el que se considere al menos lo dispuesto en los artículos 49 al 54 del Reglamento de la LFPDPPP o en el artículo 59 de la LGPDPPSO.
- Verificar que el encargado implemente las medidas de seguridad necesarias para el tratamiento de los datos biométricos.
- Corroborar que los encargados presten sus servicios atendiendo puntualmente las instrucciones de los responsables de los datos personales, pues a pesar de que el encargado que incumpla con las instrucciones del responsable deberá cumplir con las obligaciones que la normatividad impone y, en su caso, podrían ser sujetos de las sanciones que prevén la LFPDPPP y la LGPDPPSO, respectivamente, el responsable original seguirá teniendo que responder por el tratamiento indebido de los datos personales que están en posesión del encargado.

5.7 Obligaciones en torno a los derechos ARCO y recomendaciones para su cumplimiento

Fundamento legal

- Artículos 16 de la Constitución Política de los Estados Unidos Mexicanos, 22 de la LFPDPPP y Capítulo VII de su Reglamento.
- Título Tercero de la LGPDPPSO y Título Tercero de los Lineamientos Generales.

¿Cuáles son los derechos del titular?

El derecho a la protección de los datos personales permite a los individuos tener control sobre su información personal. La LFPDPPP y la LGPDPPSO reconocen los derechos de los titulares respecto del tratamiento de sus datos personales, a estos derechos se les conoce como Derechos ARCO, los cuales son:

La LFPDPPP y su Reglamento prevén la forma en que estos derechos serán ejercidos. En el mismo sentido, pero a mayor grado de detalle, la LGPDPPSO y los Lineamientos Generales, prevén los requisitos para ello. Por ejemplo, estos últimos, desarrollan el procedimiento para ejercer los derechos ARCO relacionados con personas fallecidas.

Además de estos cuatro derechos referidos internacionalmente con el acrónimo ARCO, la LFPDPPP reconoce a los titulares su derecho a revocar el consentimiento otorgado previamente para el tratamiento de su información personal, en cualquier fase del tratamiento, sin que se le atribuyan efectos retroactivos. Por su parte, la LGPDPPSO no prevé explícitamente la revocación del consentimiento; sin embargo, tienen otros derechos para solicitar que sus datos no sean tratados por el responsable, como se explicará más adelante.

Aunque la revocación del consentimiento no forma parte de los Derechos ARCO, se explica en este apartado debido a que es un derecho más que en materia de datos personales en posesión de particulares, tienen los titulares.

Por último, la LGPDPPSO prevé la prerrogativa de portabilidad, el cual faculta al titular para obtener y recibir de un responsable, en un formato estructurado y comúnmente utilizado, los datos personales tratados.

¿En qué consiste el derecho de acceso?

El titular podrá acceder a sus datos personales que obren en poder del responsable, así como a conocer el aviso de privacidad al que está sujeto el tratamiento y la información relativa a las condiciones y generalidades del tratamiento.

¿En qué consiste el derecho de rectificación?

El titular de los datos, en todo momento, tendrá derecho a rectificarlos cuando sean inexactos, desactualizados o incompletos. En otras palabras, puede solicitar a quien utilice sus datos personales que los corrija cuando los mismos resulten ser incorrectos, desactualizados o inexactos.

¿En qué consiste el derecho de cancelación?

El titular tendrá, en todo momento, el derecho a cancelar sus datos personales, es decir, a que se eliminen de las bases de datos, archivos, registros, expedientes y sistemas del responsable, a fin de que ya no sean tratados por el mismo, o cuando considere que no están siendo utilizados o tratados conforme a las obligaciones y deberes que se encuentran contenidos en la LFPDPPP o en la LGPDPPSO.

La cancelación de los datos personales no siempre procede de manera inmediata, ya que en algunos casos resulta necesaria la conservación de los mismos con fines legales y de responsabilidades. A este periodo de conservación se le denomina bloqueo y, durante el mismo, los datos personales no podrán ser utilizados para ninguna finalidad que no sean las antes señaladas y, una vez concluido, deberán ser suprimidos. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la ley aplicable en la materia.

En caso de que la cancelación resulte procedente, el responsable del sector público o privado deberá comunicar al titular, en un periodo de 20 días hábiles contados a partir de que recibió la solicitud de cancelación,[25] la determinación adoptada, a fin de que, si resulta procedente, se haga efectiva dentro de los 15 días hábiles siguientes. Una vez cancelado el dato, se dará aviso a su titular.

En materia de responsables a los que les aplica la LFPDPPP, este ordenamiento contempla en su artículo 26, las causas bajo las cuales el responsable no estará obligado a cancelar los datos personales:

- Se refieran a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
- Deban ser tratados por disposición legal;
- La cancelación obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;
- Sean necesarios para proteger los intereses jurídicamente tutelados del titular;
- Sean necesarios para realizar una acción en función del interés público;
- Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, o
- Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

[26] De conformidad con el artículo 32 de la LFPDPPP, este plazo puede ser ampliado por un periodo igual; de conformidad con el artículo 51 de la LGPDPPP, este plazo podrá ser ampliado hasta por diez días hábiles.

¿En qué consiste el derecho de oposición?

El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos personales o exigir el cese del mismo, cuando:

- Exista una causa legítima y la situación específica del titular requiera el cese del tratamiento, a fin de evitarle un daño o perjuicio, aun siendo lícito el tratamiento.
- No quiera que su información personal sea utilizada para fines específicos.

Frente a los Sujetos Obligados de la LGPDPPSO, los titulares podrán, además de los casos arriba señalados, oponerse al tratamiento de sus datos cuando:

- Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

De resultar procedente el ejercicio del derecho de oposición, el responsable no podrá tratar los datos personales del titular. Existen casos en los que el derecho de oposición no procederá, específicamente cuando el tratamiento de la información personal sea necesario para el cumplimiento de una obligación legal.

Para el ejercicio del derecho de oposición, los responsables sujetos a la LFPDPPP, podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.

¿Por qué causas puede resultar improcedente el ejercicio de derechos ARCO?

Es verdad que todos podemos ejercer nuestros derechos ARCO en cualquier momento; sin embargo, existen ciertas causas por las que puede resultar improcedente su ejercicio.

La LFPDPPP y la LGPDPPSO contemplan las siguientes:

- Cuando el titular o su representante no estén debidamente acreditados para ello;
- Cuando los datos personales no se encuentren en posesión del responsable;
- Cuando exista un impedimento legal;
- Cuando se lesionen los derechos de un tercero;
- Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;
- Cuando la cancelación u oposición haya sido previamente realizada.

Adicionalmente, la LGPDPPSO prevé, en su artículo 55, las siguientes causas por la que puede resultar improcedente el ejercicio de los derechos ARCO:

- Cuando se obstaculicen actuaciones judiciales o administrativas;
- Cuando el responsable no sea competente;
- Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
- Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
- Cuando en función de las atribuciones legales del responsable, el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o
- Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

Por su parte, el artículo 26 de la LFPDPPP prevé las siguientes causas por las cuales el responsable no estará obligado a cancelar los datos personales ante una solicitud de cancelación de un titular:

- Se refieran a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
- Deban ser tratados por disposición legal;
- La cancelación obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;
- Sean necesarios para proteger los intereses jurídicamente tutelados del titular;
- Sean necesarios para realizar una acción en función del interés público;
- Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, o
- Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Es importante señalar que, en todos los casos anteriores, el responsable deberá informar al titular el motivo de su determinación, en el plazo previsto para ello.

¿Qué es la revocación del consentimiento?

Por regla general, todo tratamiento de datos personales está sujeto al consentimiento del titular. Ahora bien, para que el control sea completo, el titular tiene el derecho de retirar el consentimiento en cualquier momento, sin que se le atribuyan efectos retroactivos.

De conformidad con la LFPDPPP, el responsable deberá establecer los mecanismos y procedimientos para que el titular pueda revocar su consentimiento. Dichos mecanismos deberán ser sencillos y gratuitos, permitir al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal, y estar informados en el aviso de privacidad.

Se deberá tomar en cuenta que existen dos modalidades en las que puede ocurrir la revocación del consentimiento:

Total

Se da sobre la totalidad de las finalidades consentidas. Esto implica que el responsable deje de tratar por completo los datos del titular.

Parcial

Ocurre sobre tratamientos determinados. En este caso, el responsable puede seguir tratando los datos personales para aquellas finalidades para las cuales el titular no revocó el consentimiento.

La LGPDPPSO no prevé explícitamente la revocación del consentimiento; sin embargo, cuando un titular no desee que sus datos personales sigan siendo tratados por un sujeto obligado, podrá ejercer su derecho de cancelación.

¿En qué consiste la portabilidad de los datos personales?

Es una prerrogativa prevista únicamente por la LGPDPPSO. Faculta al titular para obtener y recibir de un responsable del sector público, en un formato estructurado y comúnmente utilizado , los datos personales tratados que le conciernan y que sean tratados en soporte electrónico, así como el derecho de transmitirlos o solicitar sean transferidos a otro responsable, para su reutilización y aprovechamiento en un nuevo tratamiento, sin que medie obstáculo alguno por parte del responsable transferente.

¿Cómo se debe atender una solicitud de ejercicio de Derechos ARCO, revocación del consentimiento o de la prerrogativa de portabilidad?

En relación con las solicitudes de ejercicio de Derechos ARCO –y de revocación del consentimiento, en su caso- el responsable deberá:

- Establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO e informarlos a través de su aviso de privacidad.
- En el caso de responsables del sector privado, las solicitudes de ejercicio de derechos ARCO deberán tramitarse a través de la persona o departamento de datos personales designado para ello. En el caso de responsables del sector público, a través de su Unidad de Transparencia.
- Atender en tiempo y forma las solicitudes de los titulares, dando respuesta a las mismas, aunque el ejercicio no proceda.
- En caso de negativa del ejercicio de alguno de los derechos, se deberá informar al titular el motivo, en tiempo y forma, acompañando, en su caso, de las pruebas pertinentes.

Los plazos que establecen el artículo 32 de la LFPDPPP y el artículo 51 de la LGPDPPSO para atención de las solicitudes de Derechos ARCO son: 20 días hábiles para comunicar al titular la determinación de la procedencia del ejercicio del derecho, y 15 días hábiles para hacer efectivo dicho ejercicio. Estos plazos se pueden ampliar, por una sola vez, cuando exista justificación e informando de ello al titular.

Asimismo, de conformidad con la LFPDPPP, en el caso de la revocación del consentimiento, los mecanismos o procedimientos que el responsable establezca para ello no podrán exceder los plazos previstos para el ejercicio de los Derechos ARCO.

El INAI ha publicado guías en relación con los Derechos ARCO y la revocación del consentimiento, las cuales invitamos a consultar:

Documentos elaborados por el INAI en materia de Derechos ARCO y de la prerrogativa de portabilidad

1. Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO (http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf).
2. Guía práctica para ejercer el derecho a la protección de datos personales (http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf).
3. Recomendaciones para la designación de la persona o departamento de Datos Personales (http://inicio.ifai.org.mx/DocumentosdeInteres/privacidadresponsable.pdf).
4. Procedimiento para ejercer los derechos ARCO (http://inicio.ifai.org.mx/SitePages/formatos-inai.aspx)
5. Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales. (http://snt.org.mx/images/Doctos/CONAIP/SNT/ACUERDO/EXT01-23/01/2018-03.pdf)

Cabe señalar que el 12 de febrero de 2018, se publicó en el Diario Oficial de la Federación el acuerdo emitido por el Sistema Nacional de Transparencia y Protección de Datos Personales por el que se aprobaron los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, mismos que, entre otros aspectos, abordan el objeto y alcance de esta prerrogativa, reglas específicas para su ejercicio y aspectos técnicos vinculados.

¿Qué obligaciones generales derivan del ejercicio de los Derechos ARCO, de la revocación del consentimiento y de la prerrogativa de portabilidad?

- Designar a una persona o departamento de datos personales, para dar trámite a las solicitudes de los titulares y fomentar la protección de los datos personales al interior de la organización, para el caso de los particulares obligados por la LFPDPPP; los sujetos obligados de la LGPDPPSO tramitarán dichas solicitudes a través de su Unidad de Transparencia.
- No condicionar el ejercicio de alguno de los Derechos ARCO a que se ejerza previamente otro derecho, ni impedir que se ejerza un derecho por el hecho que previamente se ejerció otro. Por ejemplo, el ejercicio del derecho de rectificación no podrá estar condicionado a que previamente el titular ejerza el derecho de acceso. Asimismo, el ejercicio del derecho de cancelación no podrá limitarse por el hecho de que el titular haya ejercido el de acceso con anterioridad.
- Resguardar los datos personales de tal manera que se permita el ejercicio eficiente de los Derechos ARCO.
- Permitir acceso a los datos personales cuando proceda el ejercicio, de acuerdo con los términos establecidos en la LFPDPPP o en la LGPDPPSO.

- Dar aviso de la rectificación o cancelación solicitada por el titular a los terceros a los que se hayan transferido datos personales, a fin de que realicen lo conducente.
- Responder a las solicitudes de ejercicio de Derechos ARCO en los plazos que establecen los artículos 32 de la LFPDPPP o 51 de la LGPDPPSO.
- Los responsables sujetos a la LFPDPPP deberán determinar el periodo en el cual el titular podrá acceder a los datos personales, cuando el acceso vaya a ser en el sitio donde se encuentre la información, el cual no podrá ser menor a 15 días hábiles, según lo prevé el artículo 99 del mismo ordenamiento.
- Rectificar los datos personales cuando proceda el ejercicio, en términos de lo establecido por la LFPDPPP o la LGPDPPSO.
- Cuando proceda la cancelación: (i) establecer el periodo de bloqueo y notificarlo al titular; (ii) establecer medidas de seguridad adecuadas para el periodo de bloqueo; (iii) llevar a cabo el bloqueo en el plazo de 15 días que establece el artículo 32 de la LFPDPPP o 51 de la LGPDPPSO, y (iv) transcurrido el periodo de bloqueo, suprimir los datos personales.
- Bloquear los datos personales previa supresión y no tratar los datos personales en ese periodo, salvo con fines de almacenamiento, legales y de responsabilidad
- Eliminar los datos personales de la base de datos correspondiente cuando proceda el ejercicio de cancelación, previo bloqueo.
- Dar aviso al titular una vez que se hayan cancelado los datos personales.
- No tratar los datos personales para las finalidades correspondientes, cuando proceda el ejercicio de oposición.
- Dar respuesta a toda solicitud de Derechos ARCO, revocación del consentimiento o portabilidad, con independencia de que proceda o no el ejercicio correspondiente.
- Justificar la negativa de ejercicio de los Derechos ARCO, revocación del consentimiento o portabilidad, así como informar al titular el derecho que le asiste para solicitar al INAI el inicio del procedimiento de protección de derechos, o bien, un recurso de revisión, dependiendo de si el responsable pertenece al sector privado o público.
- Emitir una respuesta que se refiera a los datos personales que se señalaron en la solicitud del titular, y que se presente en un formato legible, comprensible y de fácil acceso.
- En su caso, informar al titular la ampliación de los plazos para dar respuesta a su solicitud.
- Ejercer los Derechos ARCO, revocación del consentimiento o portabilidad, de manera gratuita, salvo los costos de reproducción y envío que tengan lugar[27].
- Poner a disposición del titular medios remotos o locales de comunicación u otros para el ejercicio de los Derechos ARCO.
- Informar en el aviso de privacidad los medios y procedimientos disponibles para el ejercicio de los Derechos ARCO y, en su caso, de revocación del consentimiento o portabilidad.
- Establecer formularios, sistemas y otros métodos simplificados para facilitar al titular el ejercicio de los Derechos ARCO.
- Ofrecer medios que faciliten el ejercicio del derecho de rectificación.

[27] El artículo 50 de la LGPDPPSO establece que la información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples, de igual forma establece que las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.

- Acordar con el titular medios de reproducción de los datos personales distintos a los informados en el aviso de privacidad.
- Gestionar listados de exclusión para llevar un control sobre el ejercicio del derecho de oposición.
- Cuando se solicite la portabilidad y ésta implique la transferencia directa a otro responsable, ofrecer opciones como la puesta a disposición de interfaces de programación de aplicación (API, por sus siglas en inglés)[28].

Los responsables obligados de la LFPDPPP también deberán:

- Establecer mecanismos sencillos y gratuitos que permitan al titular revocar su consentimiento, al menos por el mismo medio que lo otorgó.
- No exceder los plazos que establece el artículo 32 de la LFPDPPP en los procedimientos desarrollados para la revocación del consentimiento.
- Informar al titular sobre el cese en el tratamiento derivado de la revocación del consentimiento, cuando éste así lo solicite.
- Informar a los encargados sobre la revocación del consentimiento, para que realicen lo conducente.

En relación con la portabilidad de los datos, los responsables que sean sujetos obligados de la LGPDPPSO deberán:

- Atender las solicitudes de portabilidad según lo previsto por la LGPDPPSO.
- Proporcionar al titular, cuando así sea solicitado y proceda, una copia de los datos objeto de tratamiento en un formato estructurado y comúnmente utilizado.
- Desarrollar y ofrecer al titular distintos medios que contribuyan a responder a las solicitudes de portabilidad, como herramientas de descarga directa e interfaces de programación de aplicación.
- Transferir los datos de un titular que se encuentren dentro de tratamientos automatizados, al nuevo responsable de acuerdo a lo solicitado por el titular.
- Cuando a solicitud de titular se transfieran los datos personales a otro responsable, tomar todas las medidas requeridas para garantizar que se realice de forma segura, y al destinatario correcto.
- Atender las normas técnicas, modalidades y procedimientos previstos en los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales.
- Asegurarse de que los datos personales que se proporcionan al titular o transfieran a otro responsable, no incluyan datos personales de otros titulares ajenos al solicitante.

[28] API es un conjunto de definiciones, protocolos y herramientas de subrutinas para desarrollar programas y aplicaciones. Son las interfaces de aplicaciones o servicios web puestas a disposición por los responsables para que otros sistemas o aplicaciones puedan enlazarse y trabajar con sus sistemas.

Recomendaciones específicas para la atención de solicitudes de ejercicio de Derechos ARCO, revocación del consentimiento y la prerrogativa de portabilidad en el tratamiento de datos biométricos

- Almacenar, organizar y administrar los datos biométricos de forma tal que permita la atención de las solicitudes de ejercicio de derechos ARCO, revocación del consentimiento y portabilidad en tiempo y forma.
- Establecer procedimientos o protocolos de actuación para determinar cómo se deberán atender las solicitudes de Derechos ARCO y, en su caso, de revocación del consentimiento, así como de la portabilidad, cuando el tratamiento de datos biométricos se realice por parte de terceros. Al respecto, es importante tener en cuenta que quien está obligado a dar atención a las solicitudes es el responsable del tratamiento.

5.8 Evaluación de impacto en la protección de datos personales

Fundamento legal

- Artículos 3, fracción XVI y 74 al 79 de la LGPDPPSO y 120 de los Lineamientos Generales.

¿Qué es la Evaluación de Impacto en la protección de datos personales?

Es un análisis documentado mediante el cual los responsables que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informática, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar posibles riesgos para dichos datos, con el objeto de conocer las medidas implementadas y por implementarse, para protegerlos y mitigar los riesgos identificados.

La realización de evaluaciones de impacto en la protección de datos personales es una obligación para los sujetos obligados de la LGPDPPSO cuando realicen tratamientos intensivos o relevantes, salvo ciertas excepciones previstas por el artículo 79 de la LGPDPPSO; sin embargo, la realización de estas evaluaciones es una buena práctica que se recomienda realizar para cualquier clase de responsable, sea éste del sector público o privado[29] e independientemente del tipo de tratamiento de datos personales que realice, salvo las excepciones ya señaladas.

Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la Evaluación de impacto en la protección de datos personales.

[29] Como lo prevé el artículo 48, fracción V, del Reglamento de la LFPDPPP.

De conformidad con el artículo 75 de la LGPDPPSO, se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

Cabe señalar que el 23 de enero de 2018, se publicó en el Diario Oficial de la Federación, entre otros acuerdos emitidos por el Consejo Nacional de Sistema Nacional de Transparencia Acceso a la Información Pública y Protección de Datos Personales, el Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.

Dichas disposiciones administrativas establecen el marco general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales. Asimismo, contienen criterios adicionales para determinar que se está en presencia de un tratamiento intensivo o relevante de datos personales, en función de:

- El número de titulares;
- El público objetivo;
- El desarrollo de la tecnología utilizada, y
- La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue.

Los sujetos obligados de la LGPDPPSO deberán presentar las evaluaciones de impacto a la protección de datos que realicen treinta días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique un tratamiento relevante o intensivo de datos personales, ante el Instituto o los organismos garantes.

El Instituto y los organismos garantes, según corresponda, emitirán, de ser el caso, recomendaciones no vinculantes sobre la evaluación de impacto en la protección de datos personales presentado por el responsable obligado de la LGPDPPSO, dentro de los treinta días siguientes contados a partir del día siguiente a su presentación.

Los responsables regulados por la LFPDPPP que, en su caso, decidan voluntariamente realizar una evaluación de impacto en la protección de datos personales no requerirán presentarla ante el Instituto.

En el caso de implementaciones de sistemas biométricos dentro de una organización, se recomienda a todos los responsables realizar una evaluación de impacto en la protección de datos, para determinar riesgos relacionados con el tratamiento de los datos biométricos y analizar las posibilidades de efectuar medidas para mitigar dichos riesgos. Asimismo, es importante señalar que, para realizar la evaluación de impacto en la protección de datos personales, será necesario considerar el propósito del sistema y su contexto.

Por último, este análisis puede también desarrollarse mientras el sistema opere –y no sólo previo a su implementación-, con el objeto de realizar los cambios y modificaciones cuando éstos resulten necesarios.

¿Cuáles son las obligaciones relacionados con la evaluación de impacto en la protección de datos personales?

- Los sujetos obligados de la LGPDPPSO deberán realizar una evaluación de impacto a la protección cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales de conformidad con las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.
- Los sujetos obligados por la LGPDPPSO deberán presentar la evaluación de impacto en la protección de datos personales ante el Instituto o los organismos garantes, según corresponda, 30 días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.
- No es necesario hacer la evaluación de impacto en la protección de datos personales, cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia.

Para el caso de los responsables del sector privado, la evaluación no es obligatoria sino un instrumento de autorregulación, que resulta conveniente para evitar impactos no deseados en la protección de datos personales por la implementación de nuevas tecnologías o medidas para el tratamiento.

Recomendaciones específicas para la Evaluación de impacto en la protección de datos personales cuando se trate de datos biométricos.

Cuando haya tratamiento de datos personales biométricos, se recomienda que la evaluación de impacto en la protección de datos personales incluya un análisis de los siguientes elementos:

- Si los datos biométricos resultan necesarios y efectivos para atender una necesidad en específico de la organización;
- La comparación del beneficio obtenido por el uso de los datos biométricos versus el costo por una posible violación de la LGPDPPSO, y
- La existencia de una forma menos invasiva para lograr el fin que se persigue.

Además de lo anteriormente señalado, existen otros factores que deben ser tomados en cuenta cuando se implementa un sistema biométrico, incluyendo: su localización, riesgos en la seguridad, si se hará una verificación o una identificación, número esperado de usuarios finales, circunstancias de los usuarios y datos existentes, entre otros.

Cada modalidad de biométrico tiene sus fortalezas y debilidades que deben ser evaluadas en relación con la aplicación antes de su implementación. La efectividad de un determinado sistema biométrico dependerá del tipo de tecnología que se utilice y la forma en que ésta sea usada.

Entre los puntos a considerarse para la selección de una tecnología biométrica en particular, y para la correspondiente evaluación de impacto a la protección de datos personales, pueden incluirse los siguientes:

- El medio ambiente;
- La necesidad de velocidad en la transacción;
- Los costos asociados con la obtención y almacenamiento de plantillas y reconocimientos de conductas biométricas;
- Tamaño de la población y demografía;
- Ergonomía, e
- Interoperabilidad con sistemas existentes.

6. Documentos consultados

Regulación Consultada

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en http://inicio.inai.org.mx/MarcoNormativoDocumentos/LFPDPPP.pdf
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en http://inicio.inai.org.mx/MarcoNormativoDocumentos/ReglamentoLFPDPPP_21122011.pdf
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, disponible en http://inicio.inai.org.mx/MarcoNormativoDocumentos/LEY%20GENERAL%20DE%20PROTECCIÓN%20DE%20DATOS.pdf
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, disponible en http://diariooficial.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales, disponible en http://snt.org.mx/images/Doctos/CONAIP/SNT/ACUERDO/EXT01-23/01/2018-03.pdf
- Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, disponible en http://snt.org.mx/images/Doctos/CONAIP/SNT/ACUERDO/ORD01-15/12/2017-06.pdf

Referencias

- Biometrics in the workplace. Comisionado de Protección de Datos Personales de Irlanda. https://www.dataprotection.ie/docs/Biometrics-in-the-workplace/m/244.htm
- Estudio Data at Your Fingertips Biometrics and the Challenges to Privacy, de la Oficina del Comisionado de Privacidad de Canadá, 2011, disponible en https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/
- Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report. NIST, Estados Unidos, 2014, disponible en: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf
- Guidance on Collection and Use of Biometric Data, Oficina del Comisionado de privacidad de datos personales de Hong Kong, disponible en https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

- Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Article 29 Data Protection Working Party, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf
- Opinion 3/2012 on developments in biometric technologies, 00720/12/EN, Article 29 Data Protection Working Party, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf
- Privacy & Biometrics. Building a conceptual foundation. National Science and Technology Council. Committee on Technology. Committee on Homeland and National Security, Subcommittee on Biometrics, Estados Unidos, 2006, disponible en: https://danishbiometrics.files.wordpress.com/2009/08/privacy.pdf.
- Tecnologías biométricas aplicadas a la ciberseguridad, Instituto Nacional de Ciberseguridad, España, 2016, disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf
- VILLANUEVA, DÍAS, Derechos de las nuevas tecnologías, México, Editorial Oxford, 2015.
- Working document on biometrics, 12168/02/EN, WP80, Article 29 Data Protection Working Party, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf
- Tecnologías biométricas aplicadas a la ciberseguridad. Una guía de aproximación para el empresario, Instituto Nacional de Ciberseguridad, Gobierno de España. Septiembre 2016.

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