RECOMENDACIONES DE SEGURIDAD PARA EL TRATAMIENTO DE DATOS BIOMÉTRICOS

Diciembre 2024

Directorio

Adrián Alcalá Méndez
Comisionado Presidente

Josefina Román Vergara
Comisionada

Blanca Lilia Ibarra Cadena
Comisionada

Norma Julieta Del Río Venegas
Comisionada

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

Secretaría de Protección de Datos Personales

Dirección General de Prevención y Autorregulación

Dirección de Seguridad de Datos Personales del Sector Público
Av. Insurgentes 3211,
Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán,
Ciudad de México, C. P. 04530.

Edición, diciembre de 2024

INDICE

Objetivo del documento

Este documento tiene como objetivo proporcionar información respecto a la composición de un sistema de tratamiento biométrico a fin de identificar las actividades que puede realizar dicho sistema, identificando directrices y recomendaciones específicas en función de la actividad que va a desarrollar, las cuales debe considerar un responsable de tratamiento de datos personales en caso de integrar a un tratamiento de datos personales un sistema biométrico.

1.-Definiciones

Las definiciones son retomadas del glosario de los documentos Guía para el tratamiento de datos biométricos[1], Diccionario de protección de datos personales, Conceptos fundamentales[2], Dictamen 3/2012 del Grupo de Trabajo del Artículo 29[3] y Privacy & Biometrics. Building a conceptual foundation. National Science and Technology Council. Committee on Technology. Committee on Homeland and National Security, Subcommittee on Biometrics[4].

Biometría: Método de reconocimiento de personas basado en sus datos biométricos.

Dato biométrico: Propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.

INAI o Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Muestra biométrica: Prototipo de un dato biométrico.

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.

Sistemas biométricos: Son las aplicaciones tecnológicas que permiten el reconocimiento automático de una persona a través de sus datos biométricos.

[1] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf, consultada el 27 de noviembre de 2024

[2] Disponible en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf, consultado el 27 de noviembre de 2024.

[3] Disponible en: https://www.aepd.es/documento/wp193_es.pdf, consultado el 27 de noviembre de 2024.

[4] Disponible en: https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwisuKyVm_2JAxW-JUQIHWUhJTwQFnoECBoQAQ&url=https%3A%2F%2Fwww.hsdl.org%2Fc%2Fview%3Fdocid%3D463913&usg=AOvVaw3c0Am9AbEsrjzp2gczk9Ld&opi=89978449 consultado el 27 de noviembre de 2024.

2.-Introducción

El concepto de biometría proviene de las palabras bios (vida) y metron (medida), lo que indica que se miden e identifican características propias de un sujeto, lo cual es considerado un elemento que puede hacer identificable a una persona.

Es así como, los datos biométricos pueden ser considerados datos personales debido a que contienen información concerniente a una persona física determinada y son un elemento que permite vincular información e identificar a una persona.,

Por lo que, al encuadrar en el concepto de dato personal conforme a la normativa en la materia, independientemente de si es sector público o sector privado, los Responsables o Encargados que pretendan o traten en la actualidad datos biométricos a través de medios digitales o electrónicos deberán realizar dichos tratamientos bajo las condiciones que establece la normativa en la materia.

En el caso del sector público, será conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[5] y los Lineamientos Generales de Protección de Datos Personales para el Sector Público[6], para el privado, conforme a la Ley Federal de Protección de Datos Personales en Posesión de Particulares[7] y su Reglamento[8].

En ese sentido, el INAI elaboró el presente documento que describe características y generalidades de los datos biométricos con el objeto de que el o los tratamientos que incluyan el uso de estos, sean realizados conforme a los principios, deberes y obligaciones establecidas en la normativa para el sector público.

[5] Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf, consultado el 27 de noviembre de 2024.
[6] Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018#gsc.tab=0, consultado el 27 de noviembre de 2024.
[7] Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf, consultado el 27 de noviembre de 2024.
[8] Disponible en: https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf,consultado el 27 de noviembre de 2024.

3.-Contenido

3.1.-Datos biométricos

El concepto de dato biométrico entendido como dato personal puede construirse a partir de diversas consideraciones contenidas en documentos técnicos que abordan su composición, identificando que el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29[9], define a datos biométricos como "*propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad*".

En el mismo sentido, el Reglamento General de Protección de Datos[10], en el apartado 14 de su artículo 4 dispone que los datos biométricos son "*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"*.

En el terreno nacional no encontramos una definición normativa de datos personales biométricos. Sin embargo, podemos encontrar documentos publicados por el INAI en los que se ha definido el alcance de este concepto:

- Guía para el tratamiento de datos biométricos[11] del INAI: señala que los datos biométricos son propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.
- Resoluciones: en la resolución del procedimiento de verificación identificada con el expediente INAI.3S.07.02-039/2017[12], el INAI definió a los datos biométricos como "Aquellos rasgos físicos, biológicos de comportamiento de un individuo que lo identifican como único del resto de la población como pueden ser de manera enunciativa mas no limitativa, la imagen del iris, los rasgos faciales, el patrón de voz y la huella digital".

Por lo anterior, se puede establecer que los datos personales biométricos son datos referentes a las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, que conciernen a una persona física identificada o identificable y que son medibles.

3.1.2.-Características de datos biométricos

Una vez establecido el concepto de datos biométricos, con independencia de la finalidad de su uso, el Grupo de Trabajo de Artículo 29[13] identifica las características que deben tener:

a) universales, ya que son datos con los que contamos todas las personas;
b) únicos, ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas;

---

[9] Disponible en: https://www.aepd.es/documento/wp193_es.pdf, consultado el 27 de noviembre de 2024.
[10] Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf, consultado el 27 de noviembre de 2024.
[11] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf, consultada el 27 de noviembre de 2024.
[12] Disponible en: Resolución del Procedimiento de Verificación 3S.07.02-039/2017. Disponible en: http://inicio.ifai.org.mx/pdf/resoluciones/2017/03S%2002-039.pdf, consultado el 27 de noviembre de 2024.
[13] Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_es.pdf, consultado el 27 de noviembre de 2024.

c) permanentes, ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona, y
d) medibles de forma cuantitativa.

Derivado de lo anterior, se distinguen dos tipos de técnicas biométricas:

I. Técnicas basadas en aspectos físicos y fisiológicos que miden las características fisiológicas de una persona e incluyen: comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN y análisis de los poros de la piel, etc.
II. Técnicas basadas en aspectos comportamentales que miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, etc.

3.1.2.-Tipos de datos biométricos

Una vez identificado el concepto de datos personales biométricos, es importante conocer los tipos de datos biométricos que existen, por ejemplo, el Grupo de Trabajo de Articulo 29 identifica como ejemplos de datos biométricos los que se pueden obtener a partir de la digitalización de las huellas dactilares, los modelos retínales, la estructura facial, las voces, la geometría de la mano, las estructuras venosas, fuentes de obtención ya que, incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etcétera) pueden hacer identificable a una persona.

El tipo de dato biométrico que será tratado determinará el sistema biométrico que requiere para el reconocimiento de la persona. Es pertinente señalar que cada sistema biométrico tiene sus características propias, pudiendo rescatar de la Guía para el tratamiento de datos biométricos[14] publicada por el INAI dos clasificaciones de biométricos:

1. 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.

[14] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf, consultada el 27 de noviembre de 2024.

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.

2. 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.
Geometría 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, elementos que deben ser considerados al momento de que se defina el tipo de biométrico que será integrado al sistema de tratamiento.

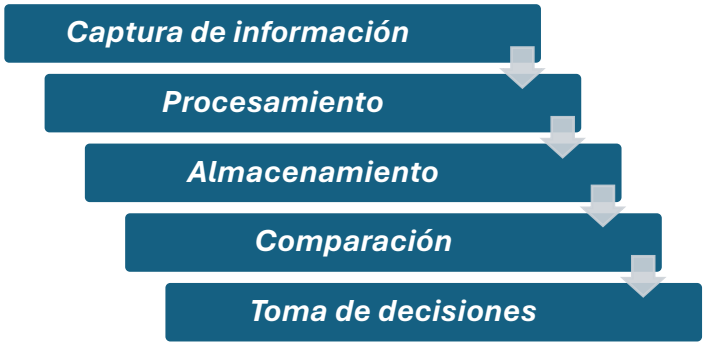
3.2.-Consideraciones para un sistema de tratamiento con uso de datos biométricos.

En la actualidad, el uso de biometría está presente en múltiples actividades de diversos sectores, buscando que este tipo de datos permita autentificar a una persona, es decir, que la persona que se presenta es quien dice ser, tratando así de evitar fraudes o suplantación de identidad.

Es así como, surge la necesidad de integrar biometría a los sistemas de tratamiento, los cuales involucran el aprovechamiento de diversas tecnologías para procesar esta información y tomar decisiones respecto al que se va a realizar con los datos obtenidos y procesados, siendo así posible establecer la existencia de sistemas de procesamiento de datos biométricos.

Dichos sistemas, se basan en recoger y procesar datos personales relativos a las características físicas, fisiológicas o conductuales de las personas físicas, entre las que cabe incluir, como se ha puesto de manifiesto recientemente, las características neuronales de estas, mediante dispositivos o sensores, creando plantillas biométricas (también denominadas firmas o patrones) que posibilitan la identificación, seguimiento o perfilado de dichas personas.

El objeto del sistema biométrico es reconocer a las personas, es decir, "volver a conocer" a una persona que ha sido registrada previamente en un sistema y encuentra una coincidencia durante la validación de información, en palabras simples, 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.



3.2.1.-Captura de información

Es el primer proceso en un sistema biométrico, este se realiza con la ayuda de hardware y software que a emplean sensores y/o aparatos que recaban una cantidad de indicadores biométricos, que son muestras que serán procesadas posteriormente, para que un indicador sea válido, debe cubrir los siguientes requerimientos[15]:

- Universal: cualquier persona posee esa característica.
- Permanente: la característica no varía con el tiempo.
- Única: la probabilidad de la existencia de dos personas con una característica idéntica es muy pequeña.
- Cuantificable: la característica se puede medir de forma cuantitativa.

[15] L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, 1998.

Por ejemplo, el documento "*Estudio sobre las tecnologías biométricas aplicadas a la seguridad*"[16] publicado por el Observatorio de la Seguridad de la Información[17] ejemplifica los siguientes parámetros considerados en cada tecnología biométrica:

- Huella dactilar con la imagen o minucia de la huella dactilar
- Reconocimiento de voz con una grabación de voz
- Reconocimiento facial con la imagen del rostro
- Reconocimiento de iris con la imagen del iris
- Reconocimiento de retina con la imagen de la retina
- Reconocimiento de la geometría de la mano con la imagen en 3-D de la parte superior y lateral de mano y dedos
- Reconocimiento de firma con la imagen de la firma y registro de medidas relacionadas con la dinámica
- Reconocimiento de escritura de teclado con el registro de las teclas pulsadas y registro de medidas relacionadas con la dinámica

3.2.2.-Procesamiento

El procesamiento incluye un algoritmo especial que selecciona características del biométrico capturado para crear una plantilla biométrica que en una primera instancia será introducida en una base de datos para que en una segunda instancia sea cotejada para reconocer la identidad de la persona con la base de datos ya generada.

Por ejemplo, el documento Estudio sobre las tecnologías biométricas aplicadas a la seguridad[18] publicado por el Observatorio de la Seguridad de la Información ejemplifica las siguientes características consideradas en cada tecnología biométrica:

- Huella dactilar con la ubicación y dirección del final de las minucias o formas de las huellas
- Reconocimiento de voz con la frecuencia, cadencia y duración del patrón vocal.
- Reconocimiento facial con la posición relativa y forma de la nariz, posición de la mandíbula
- Reconocimiento de iris con los surcos y estrías del iris
- Reconocimiento de retina con los patrones de los vasos sanguíneos de la retina
- Reconocimiento de la geometría de la mano con la altura y anchura de los huesos y las articulaciones de los dedos y de la mano
- Reconocimiento de firma con la velocidad, orden de los trazos, presión y apariencia de la firma
- Reconocimiento de escritura de teclado con la secuencia de teclas y pausas entre pulsaciones

3.2.3.-Almacenamiento

Una vez procesada la plantilla biométrica, se debe almacenar en un medio de almacenamiento adecuado para las características de la plantilla, este proceso solo se realiza una sola vez cuando se obtiene el biométrico.

---

[16] Disponible para su consulta en: https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiométricasASeguridad.pdf consultada el 27 de noviembre de 2024.

[17] Disponible en: https://observatoriociber.org/

[18] Disponible para su consulta en: https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiométricasASeguridad.pdf consultada el 27 de noviembre de 2024.

3.2.4.-Comparación

Este proceso solo puede ejecutarse cuando se cuenta con una plantilla guardada en la base del sistema, misma que 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.

En el campo de la biometría se distinguen dos tipos de comparaciones: la autenticación y la verificación.

En este proceso, es posible medir el rendimiento de un sistema biométrico a partir de cuatro características principales:

- Tasa de error de adquisición (Failure To Adquire rate): Proporción de ocasiones en las que el sistema no es capaz de capturar una muestra de calidad suficiente para ser procesada.
- Tasa de error de registro (Failure To Enrol rate): Proporción de la población para la cual el sistema biométrico no es capaz de generar muestras de calidad suficiente.
- Tasa de falso negativo (False Rejection Rate): Proporción de ocasiones en las que el sistema no vincula a un individuo con su propia plantilla biométrica existente en el registro.
- Tasa de falso positivo (False Acceptance Rate): Proporción de ocasiones en las que un sistema vincula erróneamente a un individuo con la información biométrica existente de otra persona.).

Estas características permiten que los sistemas sean catalogados como fiables y funcionales.

3.2.5.-Toma de decisiones

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 para identificarse o verificarse, o bien, un tercero.

El proceso de toma de decisiones en la biometría de acuerdo con el Estudio sobre las tecnologías biométricas aplicadas a la seguridad[19] publicado por el Observatorio de la Seguridad de la Información, consta de cuatro etapas:

- ***Búsqueda de coincidencias:*** se comparan las muestras biométricas para determinar el grado de similitud o correlación entre ellas.
- ***Cálculo de una puntuación:*** se calcula un valor numérico que indica el grado de similitud o correlación entre las muestras. Los métodos de verificación tradicionales (contraseñas, PINs, etc.) son binarios, es decir, ofrecen una respuesta positiva o negativa. Este no es el caso en la mayoría de los sistemas biométricos. La mayor parte los sistemas biométricos se basan en algoritmos de búsqueda de coincidencias que generan una puntuación. Esta puntuación representa el grado de correlación entre la muestra a autenticar y la de registro.
- ***Comparación con el umbral establecido:*** el umbral es un número predefinido, normalmente por el administrador del sistema biométrico, que establece el grado de correlación necesario para que una muestra se considere similar a otra. Si la puntuación

[19] Disponible para su consulta en: https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiométricasASeguridad.pdf consultada el 27 de noviembre de 2024.

resultante de la comparación de muestras supera el umbral, las muestras se consideran coincidentes, aunque las muestras en sí no sean necesariamente idénticas. Esto se debe a la inclusión en el análisis de las posibles deficiencias en la captura de las muestras.

- ***Decisión:*** Resultado de la comparación entre la puntuación y el umbral. Las decisiones que puede tomar un sistema biométrico incluyen: coincidencia, no coincidencia e inconcluyente (el sistema no es capaz de determinar si la muestra recogida es coincidente o no). Dependiendo del sistema biométrico implementado, una coincidencia puede permitir el acceso, una no coincidencia restringirlo y una muestra inconcluyente puede solicitar al usuario otra muestra.

Es decir, en esta fase final se determina si el sistema biométrico valida o no la identidad de una persona para ejecutar la instrucción complementaria por la que el sistema fue implementado.

3.3.-Uso de Datos Biométricos

Como se ha mencionado, en el campo de la biometría se distinguen dos tipos de tareas que puede realizar un sistema biométrico:

3.3.1- Identificación

Un sistema biométrico en el modo de identificación tiene por objeto identificar la identidad de una persona mediante la captura de ciertas características, comparando 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:

- sí en la base de datos biométricos de determinado sistema biométrico existe una muestra coincidente y
- en caso de que así sea, la identidad de la persona. Por ejemplo, un nombre o número vinculado a dicha plantilla.

De este modo se responde a la pregunta: ¿Quién es usted?

3.3.2.-Verificación

Un sistema biométrico en el modo de verificación comprueba la identidad de un sujeto, comparando la característica solo con parámetros guardados anteriormente del individuo a través de 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.

De este modo se responde a la pregunta: ¿Es usted quién dice ser?

3.4.- Recomendaciones generales

3.4.1.- Recomendaciones para desarrollos tecnológicos propios que involucren datos biométricos.

Es importante considerar diferentes aspectos a la hora de valorar el posible desarrollo de un sistema biométrico ya que, debe considerar diversos factores:

1. Es necesario incluir un sistema biométrico, debe explorar si la tarea que se va a desarrollar con el sistema biométrico puede ser realizada con otra solución que no involucre la adopción de esta tecnología.
2. 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.
3. En caso de ser inevitable la integración de un sistema biométrico, deberá identificar para que lo va a utilizar, para verificar la identidad de los usuarios (comparación 1:1) o para identificar a las personas (comparación 1: N).
4. Tratar los datos personales de acuerdo con la normatividad que regula el derecho a la protección de datos personales, en este caso, conforme a lo dispuesto en la Ley General y los Lineamientos Generales.
5. 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 utilizaran para futuras comparaciones.
6. Se debe considerar que 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, la utilización de cuatro a diez huellas dactilares resulta tan eficiente como la utilización de una sola huella dactilar de alta

calidad. Solo 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.

7. Ser conscientes de que los datos biométricos son datos personales que pueden incluir datos sensibles.
8. Evitar o limitar al máximo la recolección de datos biométricos que pudieran revelar datos sensibles no necesarios para las finalidades legitimas 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.
9. 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.
10. Solicitar siempre el consentimiento de tratamiento de datos biométricos. El sujeto obligado que recopile y trate datos biométricos debe obtener el consentimiento de la persona titular, un consentimiento expreso que debe ser informado antes de la obtención de los datos en el aviso de privacidad, donde se debe identificar la finalidad del tratamiento. De este modo no solo se cumplirá con la legislación, sino que una actuación transparente ayudará a mejorar los niveles de aceptación por la ciudadanía, la usabilidad, y, por tanto, la efectividad de estas tecnologías.
11. Facilitar el ejercicio de los derechos ARCO de los usuarios sobre sus datos personales, dándoles a conocer a las personas titulares que pueden acceder a sus datos, rectificarlos, cancelarlos e incluso oponerse a su tratamiento, siempre y cuando cumplan con el procedimiento definido y acrediten su personalidad.
12. Considerar e informar respecto a las transferencias que pueden llevarse a cabo en el aviso de privacidad, por ejemplo, cuando sean legalmente exigidas para la investigación y persecución de los delitos, así como la procuración o administración de justicia
13. Los sujetos obligados de la LGPDPPSO deberán realizar los tratamientos que estén justificados por finalidades concretas, licitas, explícitas y legitimas, 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.
14. 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.
15. Garantizar la seguridad y confidencialidad de los datos cedidos para generar confianza en los usuarios del sistema.
16. No escatimar en la adquisición de hardware y software para mejorar las condiciones del sistema biométrico.
17. Llevar a cabo divulgación de los beneficios del uso de tecnologías biométricas, desmitificando sus inconvenientes y evidenciando las mejoras que pueden suponer en el desarrollo de

actividades cotidianas, siendo transparentes del por qué se están tratando este tipo de datos a partir del trámite o actividad que se está llevando a cabo.

18. 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.
19. Revisar que la tecnología biométrica contemple mecanismos de cifrado en el almacenamiento y el tránsito de los datos.
20. Restringir el acceso a los datos biométricos únicamente a personal autorizado.
21. Guardar en bitácoras todos los accesos a los datos biométricos.
22. Evitar cruces de información innecesarios entre los sistemas biométricos y otros sistemas de tratamiento.
23. 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.
24. Minimizar el uso de bases de datos centralizadas para el almacenamiento de biométricos.
25. Contar con un sitio alterno para resguardar las bases de datos biométricos, el cual deberá estar provisto con las medidas de seguridad suficientes.
26. Considerar lo previsto por estándares internacionales, por ejemplo, los generados por el grupo de trabajo ISO/IEC JTC 1/SC 27,23[20] en donde se desarrollan aspectos de seguridad en tecnologías de la información, incluidos los relacionados con información biométrica.

3.4.2.-Recomedanciones para adopción de un sistema proporcionado por un proveedor.

Es importante considerar diferentes aspectos a la hora de valorar la posible contratación de un sistema biométrico provisto por una empresa ya que, debe considerar diversos factores:

1. Conocer la reputación de la empresa a contratar, es decir, identificar que sea una empresa reconocida, preferentemente que tenga representación en México y que no está impedida a celebrar contrataciones con entidades de gobierno en México.
2. Conocer si la empresa a contratar provee servicios complementarios o diferentes a servicios de uso y aprovechamiento de sistemas biométricos a fin de ir estableciendo cláusulas contractuales que distingan que los datos serán tratados por encargo del sujeto obligado, estableciendo la relación Responsable Encargado conforme a lo dispuesto en la norma que regula el tratamiento de datos personales.
3. Supervisar constantemente las actividades realizadas por proveedores externos que ofrezcan servicios que involucren el tratamiento de datos biométricos.
4. Identificar que el proveedor adopte estándares asociados a tecnologías biométricas, por ejemplo:
    a. Estándar ANSI X.9.84: creado en 2001, por la ANSI (American National Standards Institute) y actualizado en 2003,
    b. estándar ANSI/INCITS 358: creado en 2002 por ANSI y BioApi Consortium,

[20] Para su consulta: https://www.iso.org/committee/45306.html, consultado el 27 de noviembre de 2024

c. Estándar NIST IR 6529[21]: también conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en 1999 por NIST y Biometrics Consortium
d. Estándar ANSI 378[22]: creado en 2004 por la ANSI,
e. Estándar ISO 19794-2[23]: creado en 2005 por la ISO/IEC
f. Estándar PIV-071006[24]: creado en 2006 por el NIST y el FBI en el contexto de la norma FIPS 201[25] del gobierno de EE.UU.

5. Establecer políticas de borrado seguro una vez finalizado el contrato entre Responsable y Encargado.
6. Firmar convenios de confidencialidad con el Encargado.
7. Restringir el uso de datos.

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

3.5.- Ejemplos de uso de datos biométricos.

Como se ha mencionado, los sistemas biométricos pueden realizar dos actividades identificar cuando se busca una persona entre varios registros y validar cuando la persona es quien dice ser, en ese sentido, es posible identificar el uso de estos sistemas en actividades cotidianas:

3.5.1.- Acceso a inmuebles.

El acceso a inmuebles se realiza mediante la verificación y puede emplearse de la siguiente manera:

1. **Acceso a zonas restringidas:** en ocasiones, se requiere tener un control restringido de personal, por lo que se integran sistemas biométricos para mejorar la seguridad de un entorno.

2. **Validar hora de entrada y salida:** hay sistemas que validan el horario de arribo y desalojo de las personas a un inmueble, verificando que ellos fueron los que estuvieron físicamente en el espacio geográfico identificado.

3.5.2.-Acceso a aplicaciones.

El acceso a aplicaciones se realiza mediante la verificación y puede emplearse de la siguiente manera:

1. **Validar identidad en aplicaciones móviles para registrar en el aplicativo:** hay desarrollos informáticos que requieren validar la identidad de las personas titulares, por lo que, recaban datos biométricos para ser cotejados y validar que el usuario es humano y es quien dice ser conforme a la dinámica de registro que se respalda con la obtención de imágenes de identificaciones y muestras biométricas.

[21] Para su consulta: https://csrc.nist.gov/pubs/ir/6529/a/final, consultado el 27 de noviembre de 2024
[22] Para su consulta: https://templates.machinezoo.com/ansi378-2004 , consultado el 27 de noviembre de 2024
[23] Para su consulta: https://www.iso.org/standard/50864.html, consultado el 27 de noviembre de 2024
[24] Para su consulta: https://fbibiospecs.fbi.gov/certifications-1/faq, consultado el 27 de noviembre de 2024
[25] Para su consulta: https://csrc.nist.gov/pubs/fips/201-3/final, consultado el 27 de noviembre de 2024

2. Validación de identidad para mostrar contenido: hay aplicaciones que cifran el contenido del desarrollo, dando acceso a las personas a partir de un sistema biométrico que valida la identidad del usuario para desplegarle su información.

3.5.3.-Validación de identidad en trámites.

Esta actividad es cada vez más común y su objetivo es validar la identidad de personas, en el caso de sujetos obligados se emplea para el registro a programas sociales o a tramites diversos que brinda la administración pública, esta se realiza mediante la verificación y puede emplearse de la siguiente manera:

1. Registro a programas sociales: se generan sistemas que emplean hardware y software para poder realizar un registro y garantizar la identidad de la persona titular, esto para que entre a un proceso de inscripción y pueda acceder a programas sociales cuando cumpla con los requisitos adicionales para la obtención del beneficio.

2. Registro a plataformas para realizar trámites: se generan sistemas que emplean hardware y software para poder realizar un registro y garantizar la identidad de la persona titular, esto para que, cada que lleve a cabo un registro de trámite se garantice que es la persona registrada en el sistema.