Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

# Carrera de Especialización en Seguridad Informática

**Tema**

# Autenticación de usuarios utilizando Biometría

Autor/a:
Lic. Sergio E. Albor

Tutor/a del Trabajo Final:
Profesor Dr. Juan Pedro Hecht

Año
2021

# Índice

Declaración Jurada:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

SERGIO E: ALBOR
DNI:21.648.052
FIRMADO

# 1. Introducción

Desde antaño y continuamente los humanos utilizamos protocolos de identificación, e implícitamente de autenticación, cada vez que interactuamos con las personas de nuestro entorno. Esta forma de autenticar de una persona es llevada a cabo con tal naturalidad a diario y pasa totalmente desapercibida, por ejemplo, podemos reconocer a un amigo con solo verlo a la cara, hablar y hasta incluso escucharlo reírse.

Estas formas de identificar a las personas, que en la vida cotidiana llevamos a cabo con total naturalidad, fueron llevadas al ámbito informático para lograr **identificar fehacientemente a las personas detrás de una computadora, una tablet o un teléfono celular**, ya sea a través de sus facciones, huellas dactilares, iris, tono de voz, forma de escribir en un teclado, e incluso reconocimiento de su entorno social.

Es por eso que en este documento expondremos algunos de los métodos de identificación de usuarios más utilizados en diversos ámbitos, en relación a la autenticación.

# 2. Autenticación biométrica

La autenticación biométrica es simplemente el proceso de **verificación de la identidad de una persona** utilizando las características únicas de su cuerpo, y luego iniciar sesión en un servicio informático o electrónico, una aplicación, un dispositivo, etc.

Para lograr entenderlo mejor, la biometría es el nombre general que recibe cualquier tipo de medición calculada a través de un algoritmo que toma parámetros de diferentes puntos del cuerpo, por ej. de la cara, del dedo, del iris, etc. Esta medición **verifica que la persona es quien dice ser,** basándose en el logaritmo armado según su cuerpo. La autenticación biométrica va un paso más allá y usa esa información para compararlo con una base de datos, en donde previamente se han almacenado los datos de la persona a autenticar.

Por ejemplo, según Bontigui [1], la identificación biométrica es como un vecino que mira, a través del agujero de la puerta, a dos personas que golpearon y decide cuál de ellos es su amigo en función de la altura, el color del pelo, el color de los ojos, la voz, su color de piel, etc. La autenticación biométrica es el vecino que mira a través del agujero y, si se trata del amigo, lo deja entrar y si no es, la puerta queda cerrada.

## 3. ¿Cómo funciona la autenticación biométrica?

La autenticación biométrica funciona al comparar dos conjuntos de datos: el primero está predeterminado por el propietario del dispositivo, mientras que el segundo pertenece a un "usuario visitante" del dispositivo. Si los dos datos son casi idénticos, el dispositivo sabe que "visitante" y "propietario X" son uno, y da acceso a la persona.

**Lo importante es que la coincidencia entre los dos conjuntos de datos tiene que ser casi idéntica, pero no exactamente idéntica.** Esto se debe a que es casi imposible que dos datos biométricos coincidan al 100%. Por ejemplo, una huella puede ser ligeramente sudorosa o tener una pequeña cicatriz que cambia el patrón de impresión y si se manejara solamente por la verificación del 100% no autenticaría al dueño real de la misma.

## 4. ¿Qué función cumple la biometría?

La biometría puede cumplir dos funciones distintas, autenticación e identificación. La identificación responde a la pregunta **¿Quién es usted?**

La **identificación de un individuo** por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno a varios). Este proceso compara los datos del individuo a identificar con los datos de cada individuo en el grupo. Normalmente a través

de una base de datos centralizada que permite comparar los datos biométricos de varias personas.

Por otro lado, el proceso de autenticación/verificación responde a la pregunta: **¿Es usted realmente quien dice ser?**

La **autenticación/verificación**, por otra parte, es el proceso de probar que es cierta la identidad reclamada por un individuo. Este proceso compara sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (proceso de búsqueda de correspondencias uno a uno). Este proceso compara únicamente los datos del individuo con los datos asociados a la identidad reclamada, de tal forma que aquí no es necesario una base de datos centralizada, sino que los datos simplemente se pueden almacenar en un dispositivo descentralizado, tal como una llave o tarjeta inteligente.

**Si bien en un principio podemos llegar a pensar que la biometría puede llegar a convertirse, en el corto plazo, en el sustituto "perfecto" de las contraseñas, se han extendido una serie de "falsas creencias" en cuanto a su uso con fines de identificación y/o autenticación infalible.**

# 5. Mitos, verdades y creencias

A continuación enumeramos **catorce equívocos** en relación al uso de esta tecnología, explicando su fundamento y proporcionando referencias científicas que respaldan las aclaraciones: [2]

## 5.1 La información biométrica se almacena en un algoritmo

**El algoritmo es un método y no un medio para almacenar datos biométricos**; la información biométrica recogida (por ejemplo, la imagen de una huella dactilar) se procesa siguiendo procedimientos definidos en estándares y el resultado de ese proceso se almacena en registros de datos denominados firmas, patrones o *templates*. Estos patrones registran

numéricamente las características físicas que permiten diferenciar a las personas.

Por otro lado, hay que señalar que, para algunos tratamientos de identificación y autenticación, existen soluciones implementadas con técnicas de *Machine Learning* que contienen, en la propia aplicación y accesibles, parte de los datos biométricos utilizados para su desarrollo.

### 5.2 El uso de datos biométricos es igual de intrusivo que cualquier otro sistema de identificación/autenticación

A diferencia de una contraseña o un certificado, los datos biométricos recogidos durante un procedimiento de autenticación o identificación **revelan más información personal sobre el sujeto.**

Dependiendo de los datos biométricos recogidos, pueden derivarse datos del sujeto como su raza o género (incluso de las huellas dactilares), su estado emocional, enfermedades, discapacidades y características genéticas, consumos de sustancias, etc. Al estar implícita, el usuario no puede impedir que se recolecte esa información suplementaria.

### 5.3 La identificación/autenticación biométrica es precisa

A diferencia de los procesos basados en contraseñas o certificados, que son 100% precisos (p. ej. una clave puede ser correcta o no serlo), **la identificación/autenticación biométrica se basa en probabilidades** (por ej. una huella digitalizada proporcionará una correspondencia del 96% con un individuo). Existe una determinada tasa de falsos positivos (da por buena una suplantación) y falsos negativos (rechaza a un individuo autorizado).

Estas tasas son mayores cuanto menos preciso sea el equipo de captura de datos y dependen de las condiciones de recolección (p. ej. la luminosidad o limpieza del sensor). La precisión de algunos datos biométricos, como las huellas dactilares, también depende de la edad del individuo y es afectada por su envejecimiento.

### 5.4 La identificación/autenticación biométrica es suficientemente precisa para diferenciar siempre a dos personas

Está demostrado que el parecido biométrico entre hermanos o familiares ha confundido a sistemas biométricos.

En particular, la identidad de patrones biométricos para la identificación de hermanos gemelos, más allá del reconocimiento facial, **es un campo de estudio**. Es más, las condiciones medioambientales en entornos no controlados (por ej., el reconocimiento facial en espacios públicos, el uso de pintura facial o máscaras antivirales) provoca el **aumento de la tasa de error** y por tanto que la confusión sea más probable.

### 5.5 La identificación/autenticación biométrica es adecuada para todas las personas

Algunas personas no pueden utilizar determinados tipos de biometría porque sus características físicas no son reconocidas por el sistema.

En casos de lesiones, accidentes, problemas de salud (como parálisis) y otros, la incompatibilidad puede ser temporal. **La incompatibilidad biométrica permanente puede ser una causa de exclusión social.**

### 5.6 El proceso de identificación/autenticación biométrica no se puede burlar

Existen procedimientos y técnicas **que permiten burlar sistemas de autenticación biométrica y asumir la identidad de otra persona**.

Algunos de esos medios, como el uso de máscaras o de reproducciones de la huella NO requieren de grandes conocimientos técnicos o recursos económicos. Existen también los denominados “sistemas adversarios”, que están diseñados específicamente para tratar de engañar a los sistemas de reconocimiento de imágenes y que pueden utilizarse para burlar la identificación biométrica.

## 5.7 La información biométrica no está expuesta

A diferencia de los procesos basados en contraseñas o certificados, la mayor parte de características biométricas de una persona **están expuestas y se pueden capturar a distancia**, ya que no se oculta habitualmente el rostro, las huellas, la forma de moverse, la huella térmica, etc.

Por otro lado, aquellos sujetos que quieren burlar activamente los sistemas de seguimiento o identificación biométrica tienen recursos disponibles para hacerlo, lo que no es el caso para la gran mayoría de los ciudadanos.

Si no se toman medidas que reduzcan el riesgo de uso no autorizado de datos biométricos, su uso equivale a llevar escrito en la frente nuestras claves de acceso.

## 5.8 Todo tratamiento biométrico implica identificación /autenticación

No necesariamente, por ejemplo, el tratamiento biométrico del movimiento del ratón (mouse), utilizado para determinar si un robot está accediendo a una página web, implica tratar la información biométrica para diferenciar un humano de una máquina. Igualmente, se puede realizar un tratamiento biométrico para determinar si, en un espacio restringido, se puede diferenciar un intruso humano, un animal o un sistema de *digital signage* (proyectores que emplean tecnologías como LCD, LED, proyección y e-paper para mostrar imágenes digitales, video, páginas web, información meteorológica, menús, o texto).

Lo que existe es un **riesgo de tratar esa información**, más allá del propósito original, en el caso de que se produzca un fallo de seguridad, un cambio normativo o un tratamiento ilegítimo.

## 5.9 Los sistemas de identificación/autenticación biométrica son más seguros para los usuarios

Cualquiera de los múltiples sistemas en los que nuestros datos biométricos están siendo procesados **puede sufrir una brecha de seguridad**. El acceso no autorizado a nuestros datos biométricos en un sistema permitirá o facilitará (en el caso de utilizar múltiples factores de autenticación) el acceso en el resto de los sistemas que utilicen dichos datos biométricos.

Podría tener el mismo efecto que usar la misma contraseña en muchos sistemas distintos, por lo que la escala en la implantación biométrica es un problema en sí mismo. Y, a diferencia de los sistemas basados en contraseñas, una vez que la información biométrica ha sido comprometida, esta no se puede cancelar.

Si antes la información biométrica se almacenaba en pocas bases de datos (principalmente con fines relacionados con la seguridad pública o el control de las fronteras), ahora está almacenada cada vez en más entidades y dispositivos. Eso **aumenta enormemente la probabilidad de una brecha de seguridad** de información biométrica (durante su recolección, transmisión, almacenamiento o proceso), algo que ya está sucediendo.

## 5.10 La autenticación biométrica es fuerte

Por definición, un sistema de autenticación fuerte es aquel que exige que se proporcione, al menos, dos de los siguientes: algo que se sabe, algo que se tiene o algo que se es (biometría).

Por definición, **sólo utilizar biometría es un proceso de autenticación débil**, mientras que utilizar una tarjeta de acceso y una contraseña es un proceso de autenticación fuerte.

Aunque la autenticación biométrica muchas veces exige un proceso previo de registro o de identificación en el que, por ejemplo, en un reconocimiento facial, hay que compararlo con la foto del DNI, si, después del proceso de identificación, el proceso de autenticación sólo es biométrico, sigue siendo un sistema débil.

### 5.11 La identificación/autenticación biométrica es más cómoda para el usuario

Esta afirmación **depende de la tecnología empleada y de las circunstancias, percepción y cultura de cada usuario**. A parte de los problemas de idoneidad, pueden existir otros problemas que afecten negativamente la percepción del usuario: como ser sentimientos de invasión a la privacidad, fallos en los sistemas biométricos que impidan el acceso a los servicios, carencia de alternativas no-biométricas eliminadas o inadecuadas para dar el mismo servicio, así como la necesidad de realizar procesos de registro de datos en cada entidad.

### 5.12 La información biométrica convertida a un hash no es recuperable

Para añadir seguridad al tratamiento de la información biométrica es recomendable eliminar el patrón biométrico del que se ha obtenido el hash o biohash. Sin embargo, hay estudios que demuestran que **el hash puede ser reversible**, es decir, podría ser posible obtener el patrón biométrico original, sobre todo si se vulnera el secreto de la clave utilizada para generar el hash.

### 5.13 La información biométrica almacenada no permite reconstruir la información biométrica original de la que se ha extraído

La información biométrica almacenada (por ej. el patrón) permite reconstruir parcialmente la información biométrica original (por ej. la cara). Dicha reconstrucción parcial tiene en ocasiones la fidelidad suficiente para que otro sistema biométrico la reconozca como la original. Por ejemplo, en información biométrica facial hay estudios que demuestran que es posible conseguir desde un retrato robot una representación fiel. **La fidelidad de la**

**reconstrucción depende de la cantidad de información biométrica recogida**.

### 5.14 La información biométrica no es interoperable

Al contrario, los sistemas de tratamiento de información se desarrollan siguiendo estándares para **garantizar su interoperabilidad**.

Los sistemas que funcionan comparando el resultado de aplicar una función *hash* sobre los patrones biométricos también pueden hacerse interoperables por el sencillo método de compartir las claves utilizadas durante el proceso de hashing.

Para finalizar, podemos concluir que esta situación nos alerta de que **el uso de los datos biométricos revela más información personal sobre el sujeto que cualquier otro sistema de identificación/autenticación**, y que **la identificación/autenticación de este tipo de sistemas no es ni la más precisa ni la más segura**, ya que existen procedimientos y técnicas que permiten suplantar la identidad de los interesados de tal forma que el acceso no autorizado a datos biométricos en un sistema permite o facilita el acceso en el resto de los sistemas que utilicen dichos datos biométricos. Esto tendría el mismo efecto que usar la misma contraseña en muchos sistemas distintos y, a diferencia de los sistemas basados en contraseñas, una vez que la información biométrica ha sido comprometida, esta no se puede cancelar.

Además, **el hecho de que a día de hoy cada vez más entidades y dispositivos utilicen la biometría aumenta exponencialmente la probabilidad de que se produzca una brecha de seguridad de información biométrica**.

## 6. Biometría dactilar

Podríamos decir que los seres humanos tienen tarjetas de identificación integradas, muy fácilmente accesibles: sus huellas digitales, las cuales son

diseños virtualmente únicos, la gente tiene diminutos "valles y crestas" de piel en la punta de los dedos, estos valles y crestas se forman por una combinación de factores genéticos y ambientales aleatorios, como la posición del feto en un momento particular y la composición y densidad exacta del líquido amniótico que lo rodea lo que hace que esa huella sea única e irrepetible.

## 6.1 ¿Cómo funciona la lectura?

Hay tres tipos de lectura de huellas:

- Los lectores ópticos.
- Los lectores de capacitancia.
- Los ultrasónicos.

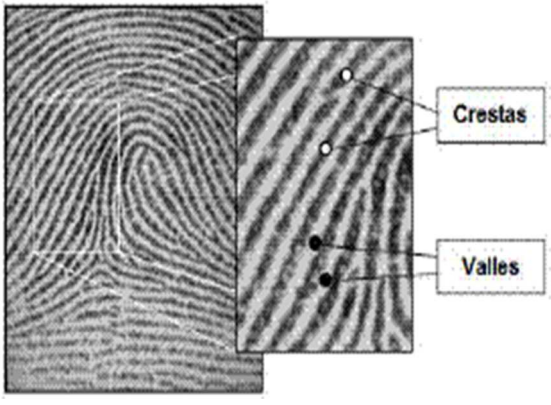
Un lector de huella digital lleva a cabo **dos tareas**:

**1)** Obtener una **imagen** de su huella digital.

**2)** Comparar el **patrón** de valles y crestas, de dicha imagen, con los patrones de las huellas que tienen almacenadas.

## 6.2 Lectores ópticos de huella dactilar

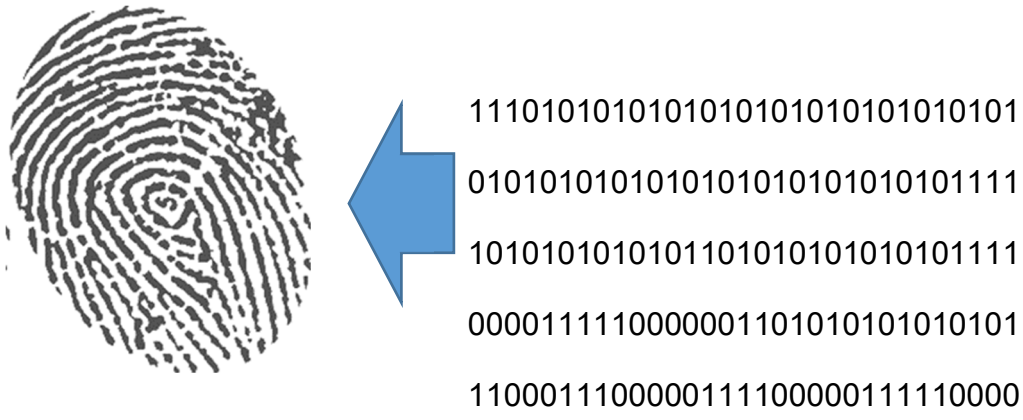
Un lector óptico funciona con un dispositivo CCD (*Charged Coupled Device* // Dispositivo acoplado de carga), [3] como el usado en las cámaras digitales, que tienen un arreglo de diodos sensible a la luz, los cuales generan una señal eléctrica en respuesta a fotones de luz. Cada diodo graba un pixel, un pequeño punto que representa la luz que le es reflejada. Colectivamente, la luz y los perfiles oscuros forman una imagen de la huella leída.




El proceso de lectura **comienza cuando el usuario pone su dedo sobre la ventana del lector**, el cual tiene su propia fuente de iluminación, típicamente un

arreglo de LED, para iluminar las crestas de la huella digital. El CCD genera, de hecho, una imagen invertida del dedo, con áreas más oscuras que representan más luz reflejada (las crestas del dedo) y áreas más claras que representan menos luz reflejada (los valles entre las crestas).

El lector toma una imagen clara y, mediante un led fotosensible, **convierte la imagen en un patrón de combinación binaria**, donde la entrada del algoritmo es una imagen de 8/16 o 32-bits en escala de grises con al menos 512 pixeles de ancho y 480 pixeles de alto y escaneado en 1.969 píxeles por milímetro o 500 píxeles por pulgada, creando un *hash* de esas imágenes que luego guardará como patrón para comprobar la identidad la próxima vez.




Antes de comparar la información obtenida con la almacenada, el procesador del lector se asegura que el CCD ha capturado una imagen clara, valida la oscuridad promedio de los pixeles, o los valores generales en una pequeña muestra, y **rechaza la lectura si la imagen general es demasiado oscura o demasiado clara**. Si la imagen es rechazada, el lector ajusta el tiempo de exposición para dejar entrar más o menos luz, e intenta leer la huella de nuevo.

Si el nivel de luz es adecuado, el lector revisa la definición de la imagen (que tan precisa es la imagen obtenida). El procesador busca varias líneas rectas que se mueven horizontal y verticalmente sobre la imagen, y si esta tiene buena definición, una línea que corre perpendicular a las crestas será hecha de secciones alternantes de píxeles muy claros y muy oscuros.

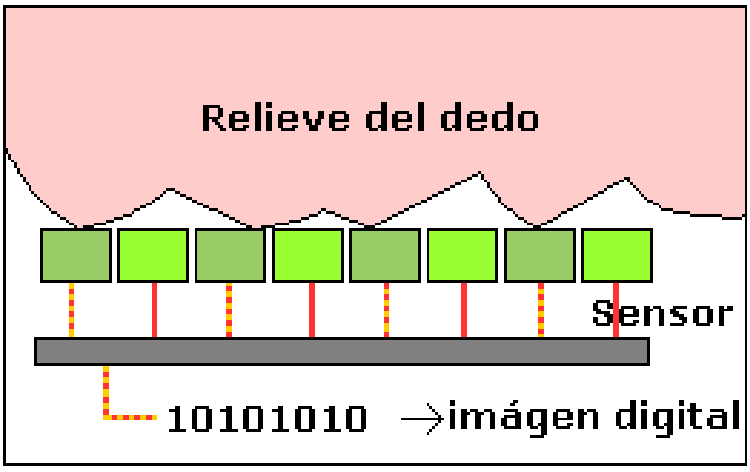
## 6.3 Lectores capacitivos de huella dactilar

Como los lectores ópticos, los lectores capacitivos de huella digital generan una imagen de las crestas y valles que conforman una huella digital pero, **en vez de hacerlo con luz, los capacitores utilizan corriente eléctrica.**

Las celdas son más pequeñas que el ancho de una cresta del dedo. El sensor está conectado a un integrador, un circuito eléctrico construido sobre la base de un amplificador operacional inversor que altera un flujo de corriente. La alteración se basa en el voltaje relativo de dos fuentes, llamado la terminal inversora y la terminal no inversora.

El procesador del lector lee esta salida de voltaje y determina si es característico de una cresta o de un valle. Al leer cada celda en el arreglo de sensores, el procesador puede construir una imagen de la huella, similar a la imagen capturada por un lector óptico.

La principal ventaja de un lector capacitivo es que **requiere una verdadera forma de huella digital y no sólo un patrón de luz y oscuridad** que haga la impresión visual de una huella digital. Esto hace que el sistema sea más difícil de engañar. Adicionalmente, al usar un chip semiconductor en vez de una unidad CCD, los lectores capacitivos tienden a ser más compactos que los ópticos.



## 6.4 Lectores ultrasónicos de huella dactilar

Se llama escáner ultrasónico porque utiliza ondas sonoras de alta frecuencia (ultrasonidos) para “mapear” el dedo en lugar de utilizar la luz como los dos lectores anteriores. Este tipo de escáner se puede integrar bajo pantallas táctiles, motivo por el cual se utiliza en algunos modelos de teléfonos celulares, pero su funcionamiento es parecido al de los escáneres ópticos en todos los efectos.

## 6.5 Análisis e integración con los softwares

En los inicios, los lectores de huella digital típicamente empalmaban varias imágenes de huellas digitales para encontrar una que corresponda. En realidad, este no era un modo práctico para comparar las huellas digitales. Una imagen borrosa puede hacer que dos imágenes de la misma huella se vean bastante diferentes, así que raramente se podrá obtener una validación correcta; además, utilizar la imagen completa de la huella digital en un análisis comparativo utiliza muchos recursos del procesador, y hace más sencillo robar los datos impresos de la huella de alguien.

En vez de esto, como dijimos anteriormente **los lectores comparan rasgos específicos de la huella digital**, generalmente conocidos como *minutiae* (minucias). Típicamente, los investigadores humanos y las computadoras se concentran en puntos donde las líneas de las crestas terminan o donde se separan en dos (bifurcaciones). Colectivamente estos y otros rasgos distintivos se llaman typica.


El software del sistema del lector **utiliza algoritmos altamente complejos** para reconocer y analizar estas *minutiae*. La idea básica es medir las posiciones relativas de la *minutiae*. Una manera simple de pensar en esto es considerar las figuras que varios *minutia* forman cuando dibuja líneas

rectas entre ellas. Si dos imágenes tienen tres terminaciones de crestas y dos bifurcaciones formando la misma figura dentro de la misma dimensión, hay una gran probabilidad de que sean de la misma persona.

Para obtener una coincidencia, el sistema del lector no necesita encontrar el patrón entero de la *minutiae* en la muestra y en la imagen almacenada, simplemente debe encontrar un número suficiente de patrones de *minutiae* que ambas imágenes tengan en común. El número exacto varía de acuerdo a la programación del lector.

## 6.6 Ventajas de un sistema biométrico de huella

Las ventajas de un sistema biométrico de huella digital consisten en que **los atributos físicos de una persona suelen ser difíciles de falsificar**, es decir, uno no puede adivinar una huella digital como adivina un *password*, no puede perder sus huellas digitales como pierde una llave y no puede olvidar sus huellas digitales como puede olvidar un *password;* es imposible tener acceso sin el patrón de una huella habilitada, incluso si interceptamos los datos desde el lector al servidor, no sabríamos con exactitud qué parte de la comunicación es una huella permitida.

Para hacer los sistemas de seguridad más confiables, una buena idea es **combinar el análisis biométrico con un medio convencional de identificación**, como ser un *password*, una tarjeta, u otro reconocimiento biométrico.

Cada día se implementan más y más nuevas soluciones con lectores de huella digitales, por su confiabilidad y seguridad. Si bien es sabido de algunos sistemas que han sido vulnerados con dedos de siliconas, con impresiones habilitadas, es difícil hacerlo sin complicidad del dueño del acceso, no obstante ello, son muchas las aplicaciones que utilizan esta tecnología, como ser sistemas de control de accesos, control de presencia de empleados, lucha contra el fraude en entidades bancarias y, muy recientemente, en algunas conocidas cadenas supermercados, han empezado a su implantación con el

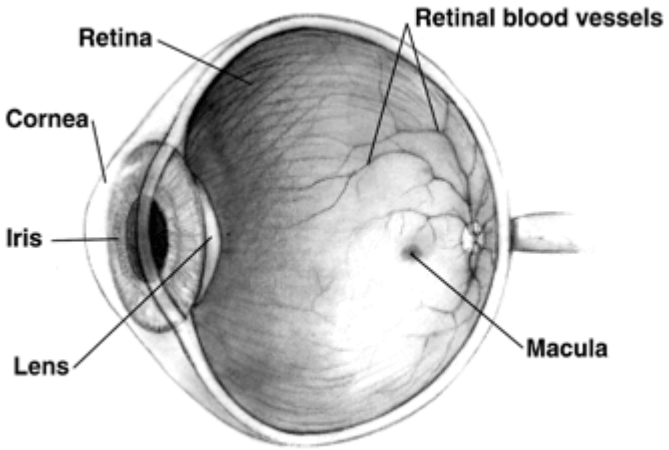
objetivo de reforzar la seguridad de sus clientes y trabajadores, evitando así robos y hurtos en sus establecimientos.

# 7. Biometría ocular

Los especialistas en seguridad consideran que **el ojo es una de las partes más confiables del cuerpo para realizar la autenticación biométrica**, ya que la retina y el iris permanecen casi sin cambios durante toda la vida de una persona.

En seguridad, el reconocimiento de iris y el escaneo de la retina son tecnologías biométricas de identificación ocular, se basan en las características fisiológicas únicas del ojo para identificar a un individuo. A pesar de que ambas utilizan alguna parte del ojo para su identificación, estos métodos biométricos son muy diferentes en su funcionamiento.

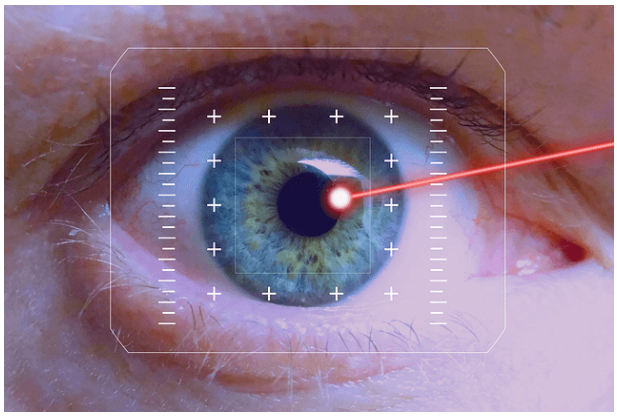
## 7.1 Escaneo de retina




La retina es la capa de tejido sensible a la luz que se encuentra en la parte posterior interna del ojo y actúa como el rollo de una cámara, impregnándose con la imagen que estamos viendo. La retina es una estructura de vasos sanguíneos tan compleja que incluso los gemelos idénticos no comparten un patrón similar. Es decir, **la retina de cada persona es única,** aunque los patrones de la retina pueden alterarse en casos de diabetes, glaucoma o trastornos degenerativos de la retina.

## 7.2 ¿Cómo funcionan los escáneres de retina?

[4]El escaneo de retina se realiza dirigiendo un rayo imperceptible de luz infrarroja, de baja energía, hacia el ojo de la persona cuando está mira a través de la pieza ocular del escáner, como quien mira por un microscopio. Ese rayo de luz traza una ruta estandarizada sobre la retina. Como los vasos sanguíneos de la retina son más absorbentes de esa luz que el resto del ojo, la cantidad de luz reflejada varía durante el escaneo. El patrón resultante de las variaciones es convertido a un patrón de código binario y se guarda en una base de datos.



## 7.3 Escaneo de Iris

El color del iris determina el color de los ojos (azul, verde, marrón, etc). El iris es una estructura fina y circular del ojo, que controla el diámetro y tamaño de la pupila y regula la cantidad de luz que penetra.

## 7.4 ¿Cómo funcionan los escáneres de Iris?

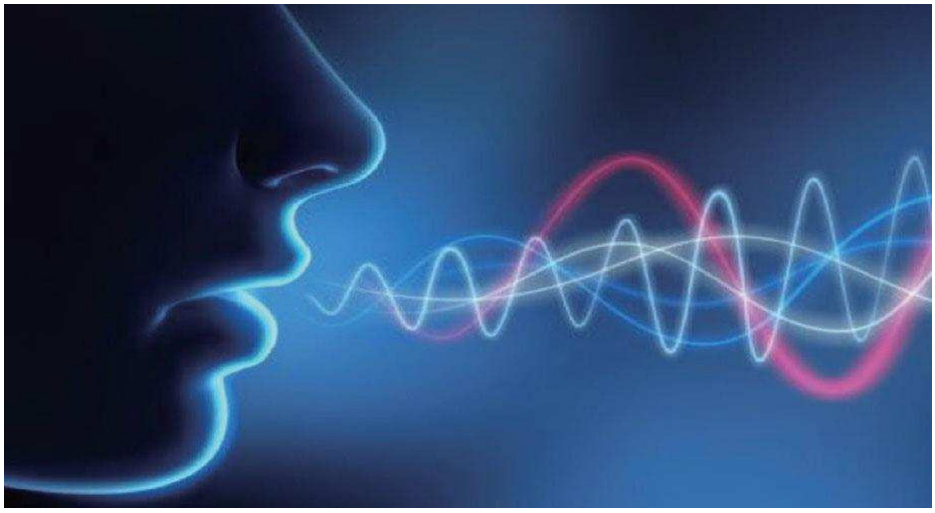
La información del iris la obtenemos a través de una cámara de alta resolución con una sutil iluminación infrarroja que captura las imágenes de la estructura del iris.

Las imágenes son convertidas en plantillas digitales y se almacenan en una base de datos en el propio lector. Estas plantillas biométricas proporcionan una representación matemática del iris, las cuales coinciden con una identificación positiva e inequívoca de una persona.

## 8. Reconocimiento de voz

El uso de la voz para autenticar personas es posible porque el aparato vocal de cada ser humano es único. Los rasgos físicos, tanto fonéticos como morfológicos (resonancia en torax, garganta y cráneo), son particulares a cada persona, lo que los convierte en inmunes a imitaciones. Esta característica da a la tecnología **ventaja sobre otros sistemas de identificación, como la introducción de un PIN.**

**Uno de los mayores problemas con el reconocimiento de voz, es lo fácil que es crear una reproducción de alta calidad de la voz de una persona**, incluso los teléfonos inteligentes de baja calidad pueden registrar con precisión la voz de un usuario y reconocerlo captando las inflexiones, tonos y acentos. Por otro lado, el reconocimiento de orador, a diferencia del reconocimiento de voz, busca identificar quién está hablando y no lo que se dice específicamente.



Para identificar al orador, un software especializado descompondrá las palabras en paquetes de frecuencias llamados formato. Estos paquetes incluyen el tono de un usuario, y juntos forman la impresión de voz del sujeto.

**Las tecnologías que utilizan la voz como principal forma de interacción irán adquiriendo un papel cada vez más relevante en los próximos años.** Las búsquedas en internet, el manejo de una *app* o controlar determinados objetos usando solo la voz ya es posible. Muchos bancos trabajan en la huella bocal como identificador único y personal para realizar pagos actualmente bancos como el BBVA, HSBC y otros están apuntando a esta tecnología para el uso de los canales móviles de pagos, haciendo caso omiso a fraudes llevados a cabo utilizando esta tecnología.

Esto no ha impedido que estas tecnologías ganen adopción general. Por ejemplo, el éxito que han logrado Amazon Echo, Google Home y otros parlantes con control de voz integrados en muchas casas inteligentes. La experiencia de autenticación biométrica de este tipo de dispositivos es increíble para los usuarios, aunque muy débil en cuestiones de seguridad.

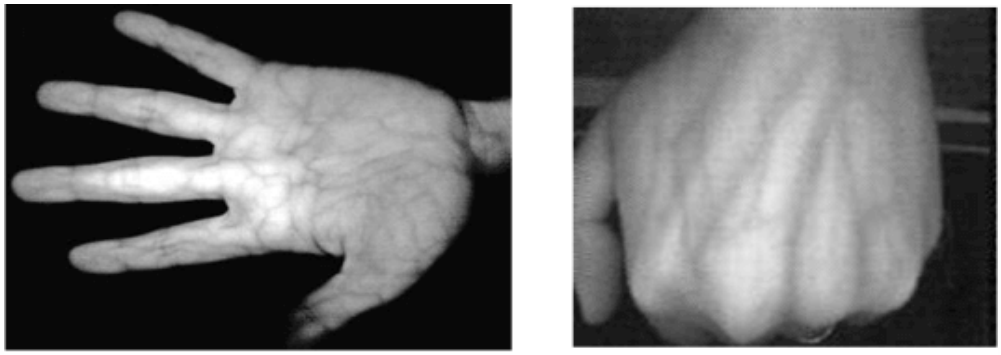
## 9. Geometría de las manos y los dedos

[5] Como el caso del de iris o los mapas tridimensionales de caras, nuestras manos son lo suficientemente diferentes de las de otras personas y eso los convierte en un **método de autenticación viable en ciertos casos**.

Un escáner de geometría de mano mide el grosor de la palma, la longitud y el ancho de los dedos, la distancia de los nudillos, etc. Las ventajas de este tipo de sistema son su **bajo costo, facilidad de uso y discreción**. También tiene algunas desventajas importantes: el tamaño de una mano puede variar a lo largo del tiempo y los problemas de salud pueden limitar los movimientos. Más importante aún, una mano no es única, por lo que **el sistema tiene poca precisión**, y, al igual que con los otros sistemas biométricos, se genera un patrón binario tomando en cuenta todas las mediciones ya nombradas.

## 10. Geometría de las venas

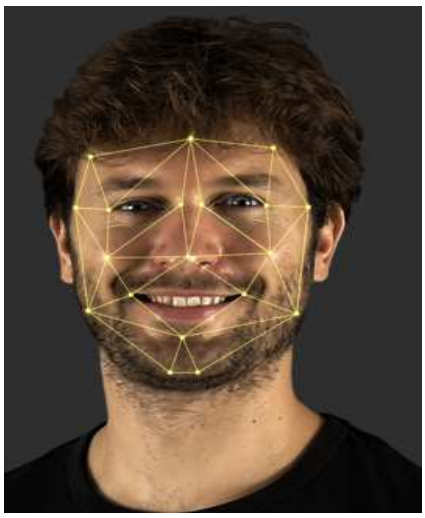
Nuestro diseño de venas es **completamente único** y ni siquiera los gemelos tienen la misma geometría, de hecho, **el diseño general es diferente de una mano a otra**. Las venas tienen una ventaja adicional ya que son increíblemente difíciles de copiar y robar porque son visibles bajo circunstancias estrictamente controladas. Un escáner de geometría de vena ilumina las venas con luz cercana al infrarrojo, lo que hace que sus venas sean visibles en la imagen.



(a) (b)

# 11. Reconocimiento facial

Es una forma de identificación biométrica que se sirve de medidas corporales, en este caso la cara y cabeza, para verificar la identidad de una persona. La tecnología recoge un conjunto de datos biométricos únicos de cada persona, asociados a su rostro y expresión facial para identificar, verificar y/o autenticar una persona.



El procedimiento de reconocimiento facial sólo necesita de un dispositivo cualquiera que disponga de tecnología fotográfica digital, cámara, para generar y obtener las imágenes y datos necesarios para crear y registrar el patrón biométrico facial de la persona a identificar; a diferencia de otras soluciones de identificación, como las contraseñas, verificación por email, imágenes, o la identificación con huella,[6] **la identificación biométrica facial utiliza patrones matemáticos únicos y dinámicos de la persona que hacen de este sistema en uno de los más seguros y eficaces.**

El objetivo del reconocimiento facial es desde la imagen entrante, encontrar una serie de datos, del mismo rostro, en un conjunto de imágenes de una base de datos. La gran dificultad reside en lograr que este proceso se realice en tiempo real.

El proceso de reconocimiento facial puede presentar **dos variantes** según el momento en el que se realice:

- Aquella en la que, por primera vez, un sistema de reconocimiento facial aborda un rostro para **registrarlo y asociarlo a una identidad**, de tal

forma que quede grabado en el sistema. Este proceso se conoce también como *onboarding digital* con reconocimiento facial.

- La variante en la que se **autentifica al usuario**, previamente registrado. En este proceso, se cruzan los datos entrantes desde la cámara, con los ya existentes en la base de datos. Si el rostro coincide con una identidad ya registrada, se concede acceso al sistema al usuario con sus credenciales.

En esta comparación de rostros, se analiza matemáticamente, y sin margen de error, la imagen entrante y se verifica que los datos biométricos se corresponden con la persona que debe hacer uso del servicio o está solicitando un acceso a una aplicación, sistema o apertura de un dispositivo para entrar a un edificio.

Gracias al uso de las tecnologías de inteligencia artificial, **los sistemas de reconocimiento facial pueden funcionar con los más altos estándares de seguridad y fiabilidad**, gracias a la integración de estos algoritmos y técnicas informáticas, el proceso puede llevarse a cabo en tiempo real.

# 12. Datos personales

## 12.01 ¿Qué son los datos personales?

Los datos personales, es información sobre personas físicas o jurídicas. Puede ser cualquier tipo de información como: datos de identidad, de domicilio, de deudas, biométrico, registro médico, etc.

## 12.02 ¿A qué datos se refiere la ley de datos personales?

A los datos personales guardados en archivos, registros, bancos de datos públicos o privados y que están guardados para dar informes.

## 12.03 ¿Mi imagen en videos de sistema vigilancia también es un dato personal?

La imagen de las personas también es un dato personal, la captura de las imágenes de una persona sin el debido aviso que esto se está realizando está penada

### 12.04 ¿Los datos biométricos son datos personales?

Sí. Los datos biométricos son un tipo de dato personal obtenido por medio de un tratamiento técnico específico. Están relacionados con las características físicas, fisiológicas o de conducta de una persona humana que permiten su identificación única.

### 12.05 ¿Qué derechos reconoce esta ley sobre mis datos personales?

La ley reconoce tu derecho a:

- Que tus datos personales no sean utilizados ni registrados sin tu consentimiento.
- Pedir y que te den la información sobre qué datos personales tuyos están registrados en bancos de datos públicos o privados.
- Pedir que tus datos sean corregidos o actualizados.
- Pedir que sean suprimidos, en los casos en que corresponda.
- Pedir que sean guardados confidencialmente.
- Iniciar acción judicial para conocer tus datos o exigir su rectificación, supresión, confidencialidad o actualización.

### 12.06 ¿Siempre es necesario mi consentimiento para que una base de datos incluya mis datos personales?

Sí. Salvo cuando:

- Tus datos fueron obtenidos de fuentes de acceso público.
- Tus datos fueron tomados para el ejercicio de funciones propias de los poderes del Estado o por una obligación legal.

- Tus datos están en listados que se limitan a datos de nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.

- Tus datos fueron obtenidos por una relación contractual, científica o profesional y son necesarios para su desarrollo o cumplimiento.

- Se trata de las operaciones que hacen las entidades financieras y de las informaciones que reciben de sus clientes.

- Un organismo público que obtuvo tus datos en ejercicio de sus funciones los cede a otro organismo público para que los use con una finalidad que está dentro de sus funciones.

# 13. Registro de datos personales

## 13.01 ¿Los datos de mi vida sexual pueden ser registrados?

Los registros de datos referidos a la vida sexual, al origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o que se relacionen con la salud, son los datos llamados ¨datos sensibles¨ y nadie puede obligarte a darlos. Tampoco pueden ser registrados, salvo que haya razones de interés general autorizadas por la ley.

## 13.02 ¿Mis datos biométricos son datos sensibles?

Todos aquellos datos biométricos que identifican a una persona son datos sensibles, sólo cuando pueden revelar otros datos y el uso de esos otros datos puede provocar discriminación. Por ejemplo, cuando los datos biométricos revelan el origen étnico o dan información sobre la salud de la persona

## 13.03 ¿Si pido conocer mis datos personales registrados en una base, ¿están obligados a darme la información?

Sobre todos tus datos registrados tenes derechos, al solicitarlos el responsable de la base de datos debe darte gratuitamente la información dentro de los 10 días corridos desde que se la solicito, siempre debe ser solicitada por escrito.

### 13.04 ¿Qué obligaciones tienen los responsables de registros de datos personales?

Además de respetar tus derechos sobre tus datos personales y darte la información que les pidas, deben exhibir los derechos que te reconoce la ley sobre tus datos personales en un lugar visible y de manera clara. Al exhibir la información sobre tus derechos, también tienen que informar que la Agencia de Acceso a la Información Pública es el organismo en el que podes hacer denuncias y reclamos para proteger tus datos personales. Toda esta información tiene que estar disponible antes de que tomen tus datos.

### 13.05 Autoridad de aplicación

**¿Quién es la la autoridad de aplicación de esta ley?**

La Agencia de Acceso a la Información Pública. Es un ente autárquico que funciona en el ámbito de la Jefatura de Gabinete de Ministros. Esta Agencia debe controlar la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados, destinados a dar informes. Debe garantizar el derecho al honor y a la intimidad de las personas y el acceso a la información.

## 14. Marco Legal de la Biometría

### 16.01 Desafíos de la biometría para la protección de los datos personales

Si hacemos un poco de historia, el principio del uso de la biometría para la identificación de las personas en Argentina inicia en [7] junio de 1966, la junta militar, autodenominada "Revolución Argentina", asumió el poder mediante un golpe de Estado. Al asumir, dictó un Estatuto de diez artículos que tenían preeminencia por sobre la Constitución Nacional. En su artículo quinto, el Estatuto arrogaba al presidente de casi todas[1] las facultades legislativas correspondientes al Congreso. Ante una realidad donde las instituciones no

[1] "Con excepción de aquellas previstas en los arts. 45, 51 y 52 para los casos de juicio político a los jueces de los
tribunales nacionales."

funcionaban de la manera en que habían sido diseñadas y la participación ciudadana era inexistente, en este contexto fue dictado el Decreto-Ley 17.671 "de identificación, registro y clasificación del potencial humano nacional". La ley atribuye las funciones del Registro Nacional de las Personas (RENAPER) respecto del procedimiento para la identificación de todas las personas domiciliadas en territorio argentino y de todos los argentinos cualquiera sea el lugar donde residan. Desde los avances de Vucetich, la sistematización del uso de huellas dactilares y la introducción del Documento Nacional de Identidad (DNI), los argentinos poco a poco fueron naturalizando su uso. La relación entre los ciudadanos y el Estado se construyó desde esa base, que luego fue ampliada hacia los actores privados.

## 16.02 La puerta de entrada a tus derechos

El mismo Registro Nacional de las Personas (RENAPER) promueve la emisión del DNI bajo la consigna de "la puerta de entrada a tus derechos", en referencia a la necesidad de contar con este documento para la realización de trámites ante el Estado, en donde prácticamente una persona no existe si no es por su número de DNI. La legislación sobre la cual está basado todo el sistema de identificación de la población se encuentra atravesada por una lógica y origen que arrastra la ideología de una dictadura militar, situación que nunca fue cuestionada política o judicialmente. Si bien es importante resaltar los defectos de forma que tiene el surgimiento de esta norma, aún más revelador es cómo se aborda el tema de fondo, la identidad de las personas. En su mismo título, la ley se refiere a las personas como "potencial humano", lo que pone la lupa sobre la concepción misma del ser humano, visto por las instituciones del Estado como un activo o recurso a disposición para ser controlado y administrado. En las cinco décadas posteriores a su sanción, el Decreto-Ley 17.671 fue utilizado por los diversos gobiernos democráticos como base para la ampliación de los sistemas de identificación de personas, justificando en el artículo 9 la legalidad de la implementación de tecnologías biométricas y procediendo, prácticamente en forma exclusiva, mediante decretos o resoluciones. El artículo 9 establece que para proceder a la identificación de las personas, el RENAPER debe recolectar “el testimonio de su nacimiento,

fotografías, impresiones dactiloscopia, descripciones de señas físicas, datos individuales, el grupo y factor sanguíneo". Así, por el Decreto 1501 de 2009, el RENAPER, organismo descentralizado bajo la órbita del Ministerio del Interior, autorizó el uso de tecnología biométrica para la emisión del DNI.[2] Posteriormente, con la Resolución 1474 de 2012 se introdujo el pasaporte biométrico.[3] En ambos casos, la principal justificación que se esgrime gira en torno a la autenticidad de los documentos que se emiten.

### 16.03 Biometría e identidad

En noviembre de 2011, a través del Decreto 1766,[4] el gobierno nacional dio vida a SIBIOS, la mayor base de datos biométricos del país, centralizada en el Ministerio de Seguridad. Según el primer artículo del decreto, el objetivo del Sistema es "prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a los fines de contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad." A partir de solicitudes de acceso a la información pública presentadas por la ADC en 2016 y 2017, el Ministerio de Seguridad estableció que los datos biométricos almacenados por SIBIOS son huellas dactilares, huellas palmares y registros de rostros. Debido a que las bases de datos existentes con anterioridad al Decreto 1766/11 se encontraban incompletas, y con el fin de poder tener los registros de los más de 40 millones de habitantes del país, el principal punto de partida para alimentar la base de datos de SIBIOS es el RENAPER, como la autoridad de la que depende la emisión del DNI y del pasaporte. La tecnología detrás de este Sistema fue adquirida a dos empresas, por parte del Ministerio de Seguridad a la francesa Morpho Safran (actualmente denominada IDEMIA), y por el lado del Ministerio del Interior a la cubana DATYS.[5] Por otra parte, debido a que SIBIOS pretende ser una base de datos federal, se determinó un esquema por el cual cada provincia pueda hacer uso del Sistema y aportar sus propios registros. Así, los Estados Provinciales pueden firmar el Acta de Adhesión con el Estado

[2] Decreto 1501 de 2009, RENAPER, Ministerio del Interior.
[3] Resolución 1474 de 2002, RENAPER, Ministerio del Interior
[4] Decreto 1766 de 2011, Ministerio de Seguridad.
[5] "La identidad que no podemos cambiar", ADC, 2017.

Nacional, a partir del cual la Superintendencia de Policía Científica de la Policía Federal procede a cargar las fichas decadactilares (correspondientes a los 10 dedos de las manos), rostros, huellas palmares y datos patronímicos que haya aportado cada Policía provincial en cuestión. Luego, para mantener el Sistema actualizado, la provincia puede realizar la incorporación de registros pertinentes directamente.


De acuerdo al artículo tercero del Decreto 1766, los principales usuarios del Sistema son: la Policía Federal Argentina, la Gendarmería Nacional, la Prefectura Naval, la Policía de Seguridad Aeroportuaria, el Registro Nacional de las Personas y la Dirección Nacional de Migraciones. A estos se suman a su vez las policías de las provincias que hayan suscrito el Acta de Adhesión. A comienzos de abril de 2017, mediante el Decreto 243,[6] se establece la ampliación de la invitación para adherirse a SIBIOS extendiéndose a "todos aquellos organismos dependientes del Poder Ejecutivo o del Poder Judicial tanto Nacionales, como Provinciales y de la Ciudad Autónoma de Buenos Aires" para que puedan formular consultas biométricas en tiempo real. SIBIOS es usado tanto con fines criminales como civiles; el primero para la investigación científica de delitos y el segundo para la identificación de personas, por ejemplo, ante catástrofes naturales o accidentes, aunque sus aplicaciones se encuentran en constante expansión. Para utilizar la base de datos de SIBIOS, los usuarios no requieren de una orden judicial. Al momento

[6] Decreto 243 de 2017, Ministerio de Seguridad.

de su lanzamiento, el gobierno nacional produjo una campaña informativa bajo el slogan "Si nos conocemos mejor, nos cuidamos más", destacando cómo ciertos rasgos de las personas sirven para identificarlas indudablemente. El video con la propaganda de SIBIOS subraya la lógica de la prevención del delito y la suplantación de identidad, destacando que gracias a este Sistema "ahora vos, sos vos". Además de las bases de datos bajo la órbita del Ministerio de Seguridad y del Ministerio del Interior mencionadas previamente, hay otras dos iniciativas estatales que desarrollaron sus propias soluciones, una en el ámbito tributario y la otra en el de seguridad social.

En 2010, la Administración Federal de Ingresos Públicos (AFIP) emitió la Resolución General 2811 creando el Registro Tributario[7], bajo el cual como parte del proceso de inscripción y otorgamiento de la Clave Única de Identificación Tributaria (CUIT), además de la Clave Fiscal con Nivel de Seguridad 3, las personas deben proceder al registro digital de la fotografía de su rostro, su firma y su huella dactilar. La Clave Fiscal es necesaria para poder realizar trámites ante la AFIP en forma online, como por ejemplo presentar declaraciones juradas, efectuar pagos, adherirse al Monotributo, solicitar la baja en impuestos o regímenes. Esto implica que un gran porcentaje de la población deba registrarse en su base de datos.

## 15. Retos y Riesgos

El uso de las computadoras y el internet abrieron el camino a riesgos de privacidad y seguridad de gran relevancia, como la compilación no autorizada de datos biométricos sin conocimiento ni consentimiento de los individuos (cámaras ocultas); la compilación biométrica con multas no necesarias para obtener una verificación contundente; el uso y distribución de los datos biométricos sin autorización o con propósitos diferentes a los autorizados, para monitorear la actividad y la expansión del sistema biométrico en áreas no pensadas desde el origen; la recopilación secreta; las tasas de aceptación falsa y de reconocimiento falso (medidas que se crean ante la probabilidad de que el sistema de seguridad biométrica acepte o rechace incorrectamente un intento

[7] Resolución General 2811, 24 de abril de 2010, Administración Federal de Ingresos Públicos.

de acceso por parte de un usuario no autorizado o autorizado, conocidos como FAR (tasa de aceptación falsa o porcentaje de instancias de identificación no autorizadas que son aceptadas incorrectamente) y FRR (tasa de rechazo falso o porcentaje de instancias de identificación autorizadas que son rechazadas incorrectamente); el robo y el fraude; la vigilancia; el reuso incompatible; el movimiento imperceptible de datos y el uso de un identificador único para conectar bases de datos

Estos riesgos están asociados con el tratamiento que se hace de los datos, el propósito para el cual estos datos son utilizados, el almacenamiento, la protección que se hace de ellos por parte de los responsables y el acceso y control de los datos por parte de sus dueños.

# 16. Ley 25.326

Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros, bancos de datos, control, sanciones y acción de protección de los datos personales.

La misma fue sancionada el 4 de Octubre de 2000 y promulgada parcialmente el 30 de Octubre de 2000.

## 16.01 Ley de Protección de los Datos Personales

[9] Disposiciones Generales

Objeto

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre,

de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

Definiciones

A los fines de la presente ley se entiende por:

— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

— Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

## 16.02 Principios generales relativos a la protección de datos

Archivos de datos – Licitud

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en su consecuencia.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

Calidad de los datos

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Consentimiento.

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

Información

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Categoría de datos.

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

ARTICULO 8° — (Datos relativos a la salud).

Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

Seguridad de los datos

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Deber de confidencialidad.

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Cesión.

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos,

al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

2. El consentimiento para la cesión es revocable.

3. El consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los supuestos previstos en el artículo 5° inciso 2;

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

Transferencia internacional.

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

2. La prohibición no regirá en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

### 16.03 Derechos de los titulares de datos

Derecho de Información.

Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

El registro que se lleve al efecto será de consulta pública y gratuita.

Derecho de acceso.

1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

Contenido de la información.

1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Derecho de rectificación, actualización o supresión.

1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

Excepciones.

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

Comisiones legislativas.

Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 23 inciso 2 por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones.

Gratuidad.

La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.

Impugnación de valoraciones personales.

1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

### 16.04 Usuarios y responsables de archivos, registros y bancos de datos

Registro de archivos de datos. Inscripción.

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas de la presente ley.

Archivos, registros o bancos de datos públicos.

1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.

2. Las disposiciones respectivas, deben indicar:

a) Características y finalidad del archivo;

b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

c) Procedimiento de obtención y actualización de los datos;

d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;

e) Las cesiones, transferencias o interconexiones previstas;

f) Órganos responsables del archivo, precisando dependencia jerárquica en su caso;

g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

3. En las disposiciones que se dicten para la supresión de los registros informatizados se está blecerá el destino de los mismos o las medidas que se adopten para su destrucción.

Supuestos especiales.

1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las

autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Archivos, registros o bancos de datos privados.

Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21.

Prestación de servicios informatizados de datos personales.

1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

Prestación de servicios de información crediticia.

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Archivos, registros o bancos de datos con fines de publicidad.

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos

para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

Archivos, registros o bancos de datos relativos a encuestas.

1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

## 16.05 ¿Quién controla? Órgano de Control

Órgano de Control.

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.

3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

Códigos de conducta.

1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

## 16.06 ¿Cuáles son las Sanciones?

Sanciones administrativas.

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de

control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Sanciones penales.

"1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

"Será reprimido con la pena de prisión de un mes a dos años el que:

1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

## 16.07 Acción de protección de los datos personales

Procedencia.

1. La acción de protección de los datos personales o de hábeas data procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

Legitimación activa.

La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

Legitimación pasiva.

La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

Competencia.

Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Procederá la competencia federal:

a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y

b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.

Procedimiento aplicable.

La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

Requisitos de la demanda.

1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo.

En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen.

2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.

3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.

4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate.

5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio.

Trámite.

1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la

recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.

Confidencialidad de la información.

1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.

Contestación del informe.

Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley.

Ampliación de la demanda.

Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o

actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.

Sentencia.

1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.

2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.

3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.

Ámbito de aplicación.

Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.

Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.

La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

El Poder Ejecutivo Nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

Disposiciones transitorias.

Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

Los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.

# • Conclusión

## Conclusión técnica

Los sistemas de autenticación basados en la biometría son:

- Prácticos.
- Presentan parámetros únicos para cada individuo.
- Imposibles de olvidarlos.
- Casi inviolables.

Más allá de lo expuesto, si tenemos en cuenta que las credenciales que se utilizan están expuestas a la vista de todos cuando hablamos, tocamos e incluso nos fotografiamos y que las mismas ante una intrusión no pueden ser modificadas, **toda esa seguridad se ve cuestionada,** incluso es necesario profundizar acerca de la calidad en los sistemas biométricos, y particularmente con la precisión de los algoritmos que estos procesos utilizan para la extracción de las plantillas de minucias e incluso con el sistema de comparación entre las mismas.

El obtener una excelente calidad en la toma de las muestras biométricas es crucial en el diseño de sistemas biométricos para el uso en la vida real. El resultado de la comparación debe ser lo más exacta y confiable posible porque muchas validaciones de la vida real se basarán en esto, en saber concretamente que (A no es B, y que A es realmente A).

Otra diferenciación que debe realizarse es la finalidad que persiguen los sistemas biométricos en sí, no es lo mismo un sistema orientado a cuestiones forenses o de control migratorio, que un sistema donde la biometría es el mecanismo elegido para corroborar una identidad para la apertura de una puerta o el fichado del presentismo en un trabajo.

En el caso del sistema orientado a cuestiones forenses o de control migratorio, la comparación biométrica es de uno a cientos o millones donde la velocidad y calidad debe ser extremadamente precisa, mientras que en el otro, es una comparación uno a uno Ej. (se tiene una huella reciente correspondiente a una

persona y se corrobora que corresponda con la existente o existentes en la base de datos para la misma persona).

El diseño y la calidad de los algoritmos obtenidos de la imagen, la extracción de características de comparación (o emparejamiento) dependen sobremanera de cuál sea el propósito del sistema, es decir a más precisión mayor certeza de confirmar esa identidad que deben ser utilizados en sistemas críticos de validación.

En algunos casos se privilegiarán la celeridad y la flexibilidad de los procedimientos de búsqueda y comparación, mientras que en otros, el énfasis estará en la precisión de la coincidencia y la baja tasa en los errores tipificados como falsos positivos y falsos negativos, simultáneamente.

Por ejemplo si hablamos de una comparación en un lector de huella dactilar de mercado para control horario realiza esta comparación de plantillas en tasas de rendimiento bajas, en cuanto a capacidad de procesamiento a razón de (1.000 huellas dactilares por segundo los mejores) en comparación con sistemas profesionales como el utilizado en el ANSES en Argentina que realiza comparaciones de 40.000 huellas por segundo.

## Conclusión marco Legal

Algo tan importante como la de validar que una persona es quien dice ser, es quien ve esa información, quien la resguarda, y quien accede a la misma.

Esto toma una gran relevancia cuando hablamos de datos biométricos, dado que estos datos ante una intrusión no pueden ser modificados.

Muchas de las aplicaciones que utilizamos de forma gratuita las pagamos con datos, y las pagamos más caras si estos datos son biométricos.

Según el sitio de argentina.gob.ar [8] al 09/2020 en argentina hay solo 5.313 bases registradas y 4.583 responsables registrados. Si tomamos en cuenta que hay registradas 565.158 medianas y grandes empresas, esto nos da menos del 1 % de estas empresas tendrían sus bases de datos registradas.

No siendo este el único aspecto a tener en cuenta, dado que se utilizan aplicaciones donde el almacenado de las bases de datos se encuentran fuera

de la legislación Argentina, y si bien existen algunos acuerdos internacionales sobre la protección de datos personales, hay mucho que se debería acordar al respecto.

Si bien la ley en la Argentina cubre varios aspectos sobre los datos personales, deja grandes huecos por cubrir o para reflexionar que es la referente a los tiempos del guardado de los datos biométricos, esta ley no menciona un protocolo o que hacer al respecto, o el tiempo que se debe guardar los logs de los accesos a la base de datos y a los diferentes sistemas de datos biométricos, para poder realizar un seguimiento minucioso de la seguridad de acceso, y poder realizar auditorías por eventuales accesos indebidos.

En resumen la ley existente pero es insuficiente en cuanto a la cobertura sobre [14] la protección que ofrece para datos personales en general y biométricos en particular, y en relación con el almacenamiento, el registro, la conservación de los datos, dejando al descubierto aspectos pendientes de tratamiento o deficitarios de la legislación actual.

## Conclusión Final

En conclusión, **el uso de la biometría puede ser un método interesante de autenticación**, mientras se combine con otras técnicas de validación como ser un One-Time Password, Token, tarjeta de coordenadas, validación cruzada, etc.

En este proyecto hemos demostrado que si bien existe una ley de datos personales los verdaderos guardianes y defensores de nuestros datos debemos ser nosotros mismos.

# Glosario

***Acceso:*** la habilidad para acceder o forma de entrada a cualquier dispositivo de un ordenador.

***Acceso remoto:*** la habilidad para acceder a una computadora desde una ubicación a distancia.

***Activo de información:*** es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones

***Almacenamiento de datos:*** Uno de los tratamientos que pueden recibir los datos.

***Bases de datos:*** una gran cantidad de información que ha sido sistematizada para su correcto almacenamiento, de forma tal que los datos que allí están contenidos puedan ser utilizados cuando se considere necesario, pudiendo ser posteriormente reordenados u organizados.

***Big data:*** en español, grandes datos o grandes volúmenes de datos) es un término que describe cualquier cantidad voluminosa de datos estructurados, semiestructurados y no estructurados que tienen el potencial de ser extraídos o tratados para obtener información.

***Biometría:*** Es la ciencia y la tecnología dedicadas a medir y analizar datos biológicos. En el terreno de la informática, la biometría hace referencia a las tecnologías que miden y analizan las características del cuerpo humano, como el ADN, las huellas dactilares, la retina y el iris de los ojos, los patrones faciales o de la voz, entre otros, a efectos de identificar personas.

***Cifrado:*** proceso para convertir información en un formato ilegible aplicando un algoritmo criptográfico que se utiliza para proteger la información de la divulgación no autorizada. Sinónimo de algoritmo de cifra. Datos biométricos: datos personales referidos a las características físicas, fisiológicas o

conductuales de una persona que posibiliten o aseguren su identificación única. Por ejemplo imágenes faciales o huellas dactilares.

***Datos informatizados:*** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

***Datos personales:*** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

***Datos sensibles:*** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

***Disociación de datos:*** Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

***Hash (código):*** bits obtenidos como resultado de aplicar una función resumen o de una sola vía a unos datos.

***Incidente:*** una ocurrencia que real o potencialmente resulte en una consecuencia adversa o amenaza para un sistema de información o la información que el sistema procesa, almacena o transmite.

***Incidente de seguridad:*** cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa u organismo.

***Información pública:*** todo tipo de dato contenido en documentos de cualquier formato que los sujetos obligados por la Ley de AIP generen, obtengan, transformen, controlen o custodien. Nube, computación en la nube: modelo de trabajo que permite ofrecer servicios de computación a través de una red que usualmente es Internet. Permite almacenar información, ficheros y datos en servidores de terceros de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red.

***Riesgos, análisis de riesgos:*** es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

***Tratamiento de datos:*** Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan en general la recolección, conservación y el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

***Titular de los datos:*** Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

***Usuario de datos:*** Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

***Vulnerabilidad:*** debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## • Bibliografía

[1] M. G. Bontigui - *Guía para la validación de los sistemas de acceso a la función pública*, 2014.

[2] V. S. Flores - Algoritmo de clasificación de huellas dactilares basado en redes neuronales función base radial - *Revista del postgrado en informática,* 2014.

[3] TEC Electrónica S.A – -2003. [En línea].

https://www.tec-mex.com.mx/promos/bit/bit0903-bio.htm

[4] U. Veracruzana - Región Xalapa seguridad de la información,» Universidad Veracruzana - [En línea] https://www.uv.mx/infosegura/general/conocimientos_autenticacion/.

[5] C. Francisco - Modelos de conducta humana para la validación de entornos inteligentes, 2015.

[6] R. M. R. Vamosi - El arte de la invisibilidad - Anaya multimedia, 2018, p. 320.

[7] https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf. tu yo digital 4-2019

[8] https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales.

[9] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[10] https://adc.org.ar/wp-content/uploads/2019/06/030-desafios-de-la-biometria-para-la-proteccion-de-datos-05-2017.pdf

[11] https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/biometria/datos-biometricos

[12] https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

[13] https://consultoria.anexia.es/blog/la-importancia-de-la-proteccion-de-datos#.YnFLT2jMLcc

[14] http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1303_MayerVI.pdf