Universidad Nacional Autónoma de México

Programa de Posgrado en Ciencias de la Administración

Investigar el robo de identidad en el sector financiero y los efectos del uso de la autenticación biométrica

TESIS

Que para optar por el grado de:

Maestro en Informática Administrativa

Presenta:
Carrillo Martínez Julio Alberto

Tutor:
Ing. M. A. René Montesano Brand
Facultad de Contaduría y Administración

Ciudad de México, diciembre de 2023

Índice

Introducción

Contexto y motivación de la investigación

La selección del tema de estudio surge a partir de una inquietud personal. En los últimos años he estado involucrado con la implementación y uso de sistemas biométricos como responsable de la tecnología utilizada para la conformación de bases de datos de identificación personal en el Instituto Nacional Electoral (INE). Esta tecnología incluye las biometrías de las huellas dactilares y del rostro, las cuales se usan en la iniciativa privada, tanto en el sector tecnológico como en el sector financiero.

El desarrollo de este estudio, denominado *Investigar el robo de identidad en el sector financiero y sus efectos con el uso de la autenticación biométrica*, pretende adentrarse en el estudio de la utilización de los rasgos físicos de las personas como medio de autenticación, los cuales son utilizados para la verificación o autenticación de las personas ante otro individuo, o ante una organización de la cual requieren servicios financieros, o de cualquier otro que precise una autenticación de identidad, con la certeza de que el resultado de esta verificación es provista por una entidad del gobierno o un tercero de confianza que registró al ciudadano y demuestra tener certeza en su identidad.

Dada mi experiencia en los últimos años, he participado en la definición técnicolegal relacionada con la protección de datos personales, en la cual se involucran las leyes por sujetos obligados o particulares; he interactuando con los responsables de alto nivel de instituciones como la Comisión Nacional Bancaría y de Valores (CNBV); he estado involucrado en la construcción de documentos como la Circular Única de Bancos (CUB) para el uso de elementos necesarios para autenticar la información biométrica con el Instituto Nacional Electoral (INE) y para conformar las bases de datos que el sector financiero tendría permitido conformar, entre ellos los bancos u otros actores del mismo sector que quisieran conformar o utilizar de forma repetida según el marco legal vigente.

Con este estudio propongo aportar una investigación que permita fundamentar la repercusión que pueda tener la implementación de este tipo de

soluciones en lo individual y en lo colectivo, para un mayor beneficio y un mejor uso, con la consiguiente cobertura de los aspectos más relevantes de la identidad, su unicidad y no alterabilidad a lo largo de la vida de cada individuo, así como los procesos y situaciones de riesgos ante el robo de identidad biométrica.

Orientación del proyecto de investigación

El tema de estudio comienza con la investigación del estado actual de los elementos de verificación de identidad que sirvan para autenticar y que el Estado ofrece. Estos elementos permiten a las instituciones o a las personas el acceso a la autenticación en términos técnicos o de verificación de los ciudadanos mexicanos en términos de la CUB, las cuales requieren el uso de alguna de las bases de datos con biometrías que el Estado ha conformado. Estas bases de datos tienen la obligación legal de conformarse y pueden identificarse, como la del Instituto Nacional Electoral (INE), la de la Secretaría de Relaciones Exteriores (SRE) y cualquier otra de la que pueda disponerse para la autenticación segura y conforme la proporcionalidad de datos personales correspondiente a la necesidad de autenticación.

A partir de los elementos con los cuales se puede confirmar la identidad de los ciudadanos mexicanos, se abordarán aquéllos generalmente utilizados para definir en qué consiste el robo de identidad en México, además de los diferentes casos y su repercusión en la sociedad, tanto en el ámbito individual como en el colectivo. El robo de identidad requiere que vayamos al fondo de las características de los servicios biométricos y de las biometrías que son utilizadas en particular en el sector financiero, lo que incluye la conformación de las bases de datos disponibles para la comparación en línea que están en poder del Instituto Federal Electoral (INE) y aquéllas que las mismas organizaciones financieras tienen la posibilidad de conformar según la regulación a cargo de la Comisión Nacional Bancaria (CNBV) y de Valores, mediante la Circular Única Bancaria (CUB).

Como parte de los marcos técnico y legal necesarios, es importante contextualizar lo que se considera robo de identidad en la industria financiera, cómo se pretende prevenir, qué mecanismos de control y verificación relacionados con la

biometría son utilizados y cómo se relacionan con las diferentes prácticas que permiten identificar los riesgos potenciales en su uso y la prevención de éstos según la regulación vigente en materia de protección de datos personales en posesión de particulares y las referencias a los casos de identificación personal y datos sensibles.

Dados los contextos tecnológico y legal actuales, se investigará la situación del uso de la verificación biométrica en el sector financiero en México, su historia, su evolución jurídica y tecnológica, y los resultados que se han obtenido de 2019 a 2022, tiempo en el cual se ha usado como un requerimiento definido por la CUB. Se abordará en la medida de lo posible cómo el sector financiero ha implementado el uso de biométricos y el cumplimiento de la legislación vigente en materia de protección de datos en posesión de particulares.

Finalmente, se hará un análisis de los resultados que ha tenido la implementación de los factores de autenticación biométricos establecidos en la regulación bancaría en la CUB. Dicho análisis se llevó a cabo en los siguientes rangos de tiempo, desde 2019 se inicia el uso de la autenticación biométrica, se establece como obligatoria, y hasta 2022, durante el proceso de implementación y los resultados que se han tenido durante cuatro años de su uso; en su caso, la implementación de procedimientos en los que las instituciones financieras asumen el riesgo al fraude mediante la verificación de dos identificaciones. La información se solicitará a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), autoridad responsable de tener medios para poder levantar quejas y reclamos ante las instituciones financieras. La periodización ya señalada permitirá comparar la efectividad de estos mecanismos han tenido en la evolución del número de casos de robo de identidad reportados. Como ya fue señalado, se trabajó con la información pública disponible de las dependencias responsables de recabar la información del objeto del estudio.

Propósito, planteamiento del problema y plan de acción del proyecto

El propósito general del proyecto es contribuir en la medida de mis posibilidades profesionales a investigar la efectividad de las medidas propuestas y si la regulación ha sido suficiente para poder contribuir en la prevención y, por ende, en la reducción de la incidencia de los casos de robo de identidad reportados.

Se requiere certeza en la verificación de la identidad de las personas/ciudadanos y del Estado mediante las diferentes instituciones, leyes y reglamentos en la materia, como lo establecido en la Ley General de Población, la cual ha requerido que se recolecten los datos personales biográficos de los ciudadanos mexicanos, que en términos generales y de manera simplificada, tiene un proceso en el registro de la identidad, entendido éste como aquella serie de actividades que de manera articulada por una autoridad oficial o reconocida permite revelar la identidad de una persona. Consiste en cinco pasos o subprocesos principales: captación de datos personales, transmisión de información, procesamiento de datos/verificación de unicidad, registro y generación de identidad, y acuse de aceptación del registro.

Dada la digitalización de los procesos y el uso de las redes de internet, los procesos se pueden llevar de manera presencial o remota, por lo que siempre existe en la verificación de identidad un primer registro almacenado, en el cual siempre consta que la persona que se ha registrado es quien dice ser. Esto ha sido verificado por una entidad con atribuciones pertinentes y los datos con los cuales se ha identificado le pertenecen, para lo cual se han extendido el uso de las bases biométricas para garantizar la unicidad de los registros y que no exista otra persona con la misma información biométrica, con ésos o con otros datos.

Planteamiento del problema

La verificación de identidad trata de resolver un problema vigente relacionado con la usurpación de ésta y el cual involucra el ciclo de vida de la información relacionada en ella, desde su registro oficial ante una entidad reconocida con la función específica de verificar la identidad con los elementos suficientes y con la

documentación necesaria, que podría incluir el nacimiento, la situación y hasta la muerte o desaparición de los individuos. En México, los registros civiles de las entidades tienen la obligación de mantener el registro documental; sin embargo, éste no se puede asociar de manera inequívoca con los elementos distintivos únicos de una persona, como sus datos biométricos, o con otro rasgo que lo puede identificar con la menor falla posible.

El Registro Nacional de Población (Renapo) es responsable de generar y proporcionar un identificador único a los ciudadanos mexicanos denominado Clave Única de Registro de Población (CURP); sin embargo, al igual que lo que sucede con los registros civiles, este identificador no puede garantizar que quien lo presente como identificador corresponda de manera inequívoca a esa persona, ya que no existen medios de validación de la identidad.

Finalmente, está el Instituto Nacional Electoral (INE), con un enrolamiento de ciudadanos mexicanos mayores de 18 años, quienes tienen que presentar elementos documentales que los acrediten como ciudadanos mexicanos que son mayores de 18 años y que habitan en un domicilio en la república mexicana o en el extranjero, y que al momento de verificar estos datos, se obtienen información biométrica facial y 10 huellas dactilares que permiten registrarlos en la base de datos y garantizar con una alta probabilidad que al registro de esta persona se le puede asociar una identidad única, con la cual va poder emitir un solo voto, gracias a la gestión de su identidad biométricas y la comparación que se hace con los registros disponibles en el padrón de electores en posesión de dicho instituto.

El padrón de electores mantiene la base datos biométrica más amplia en México y mantiene cierta posibilidad de asociación a los datos de nacimiento de los registros civiles y del Renapo mediante el uso de la CURP en todas las bases mencionadas, lo que permite contar y tener trazabilidad de la identidad a la cual el Estado está obligado a entregar y garantizar la misma, lo cual podría generar áreas de oportunidad; sin embargo, esto queda fuera del alcance de este análisis.

Desde la perspectiva institucional del Estado mexicano se ha abordado cómo se ofrece y garantiza que cada ciudadano tenga una identidad sobre la cual se

tienen derechos y obligaciones. Toca ahora abordar la perspectiva individual del ciudadano.

El ciudadano y su identidad son referentes de los diversos problemas que existen en cuanto a situaciones presenciales; con mayor razón los que se presentan en una era digital en lo relativo a la protección de la identidad y los posibles delitos asociados a su obtención y uso sin autorización.

Los diferentes tipos de relaciones personales conllevan la necesidad de identificar a las personas con las que nos asociamos. Esto no siempre es tan certero como se espera y está abierto a riesgos al saber con certeza la identidad de terceros y al proveer información de forma segura sin que sea utilizada para otras actividades no determinadas en la relación. Esto lleva a una pregunta obligada: ¿estamos seguros de que sabemos con quiénes nos relacionamos y a quiénes le proporcionamos información?

Lo mencionado anteriormente está asociado con las personas físicas; sin embargo, en el caso de las empresas o personas morales de cualquier índole que prestan servicios y cuyos pagos se hacen mediante crédito o documentos en los cuales existe una promesa de pago, y ante el creciente robo de identidad, la necesidad de verificación de identidad es irrevocable. Es necesario prevenir las posibles afectaciones derivadas de fraudes cuando se lleva a cabo el robo de identidad.

Como ya se ha mencionado, la identidad es parte intrínseca de un individuo. Y si hablamos de elementos para autenticar a una persona, hablamos de tres de ellos que pueden ser utilizados para la autenticación: *lo que sé*, algo que yo introduje y no comparto, con la finalidad que se almacene y proteja, con la finalidad de reducir la posibilidad de que alguien lo utilice sin autorización; *lo que tengo*, elementos que están en mi posesión y que protejo y no comparto, con la finalidad de que nadie pueda hacerse pasar por mí ni obtener algo al presentar este elemento como si fuera yo el requirente; finalmente y no menos importante, *lo que soy*, presentar físicamente alguna característica de mi persona, como *huellas*, *rostro/cara*, *voz*, *iris*, algo que soy y que no se puede compartir.

Una vez descritos, los elementos de seguridad *lo que sé* y *lo que tengo* pueden ser sustituidos y establecer estrategias que permitan impedir su réplica y uso de manera no autorizada, y mitigar el riesgo en su utilización de forma fraudulenta. Pero *lo que soy* no se puede cambiar ni alterar para poder mitigar su réplica en caso de que se duplique/clone, ya que no es transferible ni compartible; su perdida implica un riesgo mayor y, al ser vulnerado, es muy complicado el repudio en su utilización, ya que este último elemento está asociado a un consentimiento pleno en el uso de las características físicas que son tomadas para comprobar la identidad.

El problema planteado está relacionado con que el Estado, mediante la regulación al sector financiero, ha establecido que los usuarios de los servicios financieros, al momento de identificarse, tengan que utilizar las biometrías de huella (dedos índice derecho e izquierdo) o el reconocimiento facial que el INE o cualquier otra entidad del gobierno solicite, almacene y disponga para cotejo, para poder comprobar la identidad.

Pregunta de investigación

¿Del uso de la autenticación biométrica se ha derivado que la autenticación de los usuarios de los servicios financieros sea suficiente para tener certeza de que quien requiere un servicio es quien dice ser, pero también permite determinar de manera inequívoca un posible robo de identidad y, en consecuencia, repercute en la incidencia de los delitos de robo de identidad?

Hipótesis

La autenticación biométrica ha disminuido el porcentaje de casos de robo de identidad que se presentan en relación con la cantidad de operaciones de autenticación que se realizan en el sector financiero mexicano y su efecto corresponde a un menor número de casos.

Variables

Variable	Tipo	Descripción
Autenticación biométrica por usuario.	Independiente (x_1)	Operación de autenticación por cada usuario servicios financieros.
Casos robo de identidad.	Dependiente (y_1)	Casos reportados y catalogados por la autoridad como robo de identidad.
Porcentaje de casos robo de identidad con relació**n a** las operaciones de autenticación.	Dependiente (y_2)	Porcentaje de casos de robo de identidad reportados ante la autoridad con relación a la cantidad de operaciones de autenticación de identidad.

Comprobación de operación

Resultado de autenticación de identidad (x_1) entre los casos de robo identidad (y_1), disminuye el porcentaje de casos de robo de identidad reportados con relación al total de operaciones (y_2).

Objetivo general

Investigar los mecanismos de autenticación biométrica en el sector financiero mexicano, relacionado con los resultados obtenidos desde 2019, cuando la Comisión Nacional Bancaria y de Valores hizo obligatorio su uso, y hasta 2022, con la información disponible en la materia.

Objetivos particulares

Calificar si el uso de los mecanismos de autenticación biométricos en el sector financiero mexicano permite la autenticación plena de los ciudadanos en el proceso de contratación y, al ser clientes, el uso sostenido de dichos mecanismos provee el nivel de seguridad y certeza inicial. Asimismo, si esta autenticación ha sido suficiente para los bancos en el tiempo y permite que los solicitantes sean

identificados de manera confiable y con la mayor certeza posible de manera sostenida siguiendo los indicadores disponibles.

Analizar si el resultado de la autenticación biométrica permite al sector financiero mexicano entregar los bienes y servicios, contribuye a reducir los riesgos de un posible robo de identidad a los solicitantes al proporcionar su información biométrica, poder recibir el servicio o bien solicitado sin repudio alguno de las autorizaciones dadas por el interesado o, en su caso, negar el acceso a los servicios con el paso del tiempo.

Establecer el comportamiento del robo de identidad en relación con el uso de los datos biométricos de los ciudadanos mexicanos cuando se utilizan servicios financieros que les requieren proporcionar huellas o reconocimiento facial.

Capítulo 1. Marco teórico

En este capítulo se aborda la situación actual de la autenticación y verificación de personas para la obtención de productos y servicios financieros, su contexto legal y la situación en otros países: cómo han afrontado este reto de autenticar con certeza a sus clientes o prospectos.

1.1 Identidad en el sector financiero en México

En la contratación de los servicios financieros, las regulaciones correspondientes establecen una serie de requisitos que deberá cumplirse para asegurarse de que el contratante es quien dice ser. Estos requisitos requieren la presentación de documentos tanto personales como aquéllos que permiten acreditar el domicilio.

El termino *identidad de la persona* se ha incluido en los derechos fundamentales de la siguiente forma: “Tener un nombre y los apellidos de los padres desde que nazca, así como ser inscrito en el registro civil”. Y en la Constitución Política de los Estados Unidos Mexicanos se establece en su artículo 4 que “Toda persona tiene derecho a la identidad”.

En lo que respecta a la identidad, los documentos generalmente aceptados para acreditarla son aquéllos que tienen que ver con la inscripción a los servicios que brinda el Estado, tales como la credencial para votar, el pasaporte y la licencia de conducir, entre otros. Todos ellos cuentan con ciertos elementos de seguridad que se pueden considerar suficientes en el contexto en el que se usan.

El gobierno mexicano ha intentado crear un documento que acredite plenamente la identidad de los ciudadanos mexicanos y esta responsabilidad fue encargada al Registro Nacional de Población (Renapo); sin embargo, su aplicación no ha sido posible. Y mientras esto sucede, el gobierno ha determinado que la credencial para votar sea el documento que cumpla esa función.

Durante muchos años, la ausencia de elementos solidos de verificación de identidad ha permitido que los delincuentes puedan usurpar la identidad de otras personas y de esta forma obtener beneficios; razón por la cual el análisis que se

abordará en este documento permite adentrarse en las situaciones pasada, presente y futura, y con el uso de datos biométricos al momento de solicitar servicios financieros.

En cuanto a la verificación de identidad, existe un capítulo legal adicional que se tiene que abordar siempre en relación con la protección de los datos personales y sus diferentes características para los clientes que otorguen el consentimiento para el tratamiento de esos datos. En este caso, la Ley de Protección de Datos refiere dos tipos de datos en posesión de particulares. Éstos son:

1. *Datos personales.* Se refiere a cualquier información concerniente a una persona física, identificada o identificable.
2. *Datos personales sensibles.* Son datos personales que afectan la esfera más íntima de su titular; en este caso, los datos biométricos, los cuales se incluyeron desde 2022.

Para el tratamiento de estos datos se debe considerar el consentimiento correspondiente: “El responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales, la solicitud de consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informe en el aviso de privacidad” (INAI, 2016, 2018).

Para poder hacer uso de la verificación de identidad, invariablemente se debe obtener el consentimiento de los titulares; por su parte, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) será la entidad responsable de la protección de los datos personales y el Instituto Nacional Electoral (INE) sólo es una instancia que permite proteger y proporcionar un mecanismo de verificación de identidad, en ausencia de la cedula única de identidad. Al cumplir con estos elementos, se cuenta con la certeza jurídica de los diferentes actores que podrían participar en la verificación de identidad. Ahora corresponde a las medidas tecnológicas poder integrar y ofrecer soluciones de vanguardia para dicha verificación; contar con la mayor certeza de que la identidad de cada persona es única e intransferible y que ésta sea resguardada para

garantizar su uso correcto. Se ha caracterizado por asociarse elementos que son propios para cada persona, incluso tienen una alta probabilidad de ser únicos.

A continuación, se presentan los artículos que son parte de la Circular Única de Bancos y que expresan los requisitos que es necesario cubrir para la apertura de una cuenta bancaria, y los cuales están asociados con los elementos de identidad antes referidos:

Capitulo II

Integración de expedientes de crédito y datos de identificación de clientes.

Sección Segunda

Datos de los clientes.

Apartado A

De la identificación y realización de operaciones presenciales.

Artículo 51 Bis.- Las Instituciones deberán requerir a las personas físicas que de manera presencial soliciten la celebración de operaciones pasivas relacionadas con las Cuentas Bancarias Nivel 4, o bien operaciones activas o de servicios o medios de pago que estén relacionados con Cuentas Bancarias representación de terceros, que proporcionen de la persona que se presenta y, en su caso, de la persona a la que representa, lo siguiente:

I. Tratándose de personas físicas de nacionalidad mexicana, cualquiera de las siguientes:

a) Credencial para votar expedida por el Instituto Nacional Electoral en el país o a través de las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero.

Las Instituciones deberán efectuar las acciones de verificación a que alude el Artículo 51 Bis 4, fracción I de las presentes disposiciones respecto de las personas que se presenta y, en su caso, de la que representa en este último supuesto, no se verificará en línea la huella dactilar del representado.

…

II. Clave Única de Registro de Población. Las Instituciones deberán corroborar de manera remota con el Registro Nacional de Población que los datos proporcionados coinciden con los de dicho Registro, previamente a la contratación, de lo cual conservaran evidencia.

…

Articulo 51 Bis 2.- Las Instituciones, en sustitución a lo requerido por los Artículos 51 Bis y 51 Bis 1 de las presentes disposiciones en materia de identidad, podrán conformar una base de datos de información biométrica de sus clientes, observando los requerimientos técnicos previstos en el Anexo 71 de las presentes disposiciones, a fin de utilizarla para la verificación de la identidad de sus clientes en la celebración de contratos para realizar operaciones pasivas relacionadas con Cuentas Bancarias Nivel 4; operaciones activas o de servicios, o en la solicitud de medios de pago, relacionados con Cuentas Bancarias 3 y 4, así como para hacer retiros de efectivo y transferencias de recursos con cargo a Cuentas Bancarias Nivel 4.

Lo anterior, siempre que las Instituciones realicen, para la integración de dicha base de datos, la verificación de la coincidencia de la información biométrica del cliente con los registros biométricos del Instituto Nacional Electoral, de la Secretaría de Relaciones Exteriores u otra autoridad financiera o fiscal mexicanas, o dependencia federal, que provea un servicio de verificación de información similar al de dicho instituto (Circular Única de Bancos, s/f).

Apartado B

De la identificación no presencial

Articulo 51 Bis 6.- Las Instituciones en la identificación de sus clientes o solicitantes que sean personas físicas mexicanas o personas morales mexicanas, para la celebración no presencial de contratos: (a) apertura de Cuentas Bancarias Nivel 4; (b) de créditos al consumo para clientes o solicitantes que sean personas físicas relacionadas con Cuentas Bancarias Nivel 3 y 4, y (c) de créditos comerciales para clientes o solicitantes que sean

personas físicas con actividad empresarial o personas morales relacionados con Cuentas Bancarias Nivel 3 y 4, deberán ajustarse a lo dispuesto por el presente artículo 51 Bis 6, así como a lo dispuesto por los artículos 51 Bis 7 u 51 Bis 9 de estas disposiciones.

Para efectos de las contrataciones a que se refiere el párrafo anterior, las instituciones deberán verificar la coincidencia de la información biométrica que obtengan del cliente o solicitante, con los registros del Instituto Nacional Electoral, la Secretaría de las relaciones exteriores u otra autoridad financiera o fiscal mexicanas o dependencia federal que provea un servicio de verificación de información biométrica similar al de dicho instituto o la referida Secretaría, o con aquellas bases de datos biométricos que hayan desarrollado las propias instituciones de conformidad con lo previsto en los Artículos 51 Bis 2 y 51 Bis 3 de las presentes disposiciones.

En caso de que la información biométrica a que se refiere el párrafo anterior sean las huellas dactilares del cliente o solicitante, las Instituciones deberán asegurarse que las aplicaciones o medios de que dispongan aseguren que la huella dactilar se obtenga directamente del cliente o solicitante, es decir, prueba de huella viva, evitando el registro de huellas provenientes de impresiones en algún material que pretenda simular la huella de otra persona o de imágenes que persigan tal fin, y contar con medidas de seguridad que garanticen que la información almacenada, procesada o enviada a través de dichas aplicaciones o medios no sea conocida ni utilizada por terceros no autorizados, así como verificar que la huella dactilar que se obtenga del cliente o solicitante que presenta la credencial para votar expedida por el Instituto Nacional Electoral en el país o a través de las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, el pasaporte mexicano expedido por la Secretaría de Relaciones Exteriores en el país o a través de sus oficinas consulares en el extranjero, o la matrícula consular expedida por las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, coincidan, al menos, en un noventa por ciento con los registros de las bases de datos de dicho Instituto o de la referida

Secretaria u otra autoridad financiera o fiscal mexicanas, o dependencia federal que provea el servicio de verificación de información biométrica.

Asimismo, se requiere la información de la credencial:

a) El Código Identificador de credencial (CIC) o, en su caso, el OCR de la credencial del IFE/INE.

b) Año de registro.

c) Clave de elector.

d) Número y año de emisión.

e) Se deberán verificar los apellidos paternos, maternos y nombre(s), tal como aparezcan en la credencial y que este mismo dato coincida con el del Registro Nacional de Población (Renapo).

La regulación de los bancos permite la autenticación de sus clientes y posibles clientes de manera presencial y no presencial, como ya se ha revisado anteriormente, y requiere la verificación biométrica y una prueba de vida al momento de tomar estas biometrías. Asimismo, el anexo 71 de la CUB define los elementos técnicos con los cuales se deberán tomar.

A manera de resumen, la definición que da la Condusef a la identidad la constituyen los datos personales: nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y seguridad social, incluyendo información financiera o médica, así como cualquier otro que permita identificar a una persona (Condusef).

Para el presente estudio, identificar la información que se utiliza para asociar la identidad del cliente financiero a la identidad de la persona con la información provista por los entes del gobierno permite una protección jurídica en ambos sentidos.

1.2 Descripción del robo de identidad

Según la Condusef, la definición de robo o usurpación de identidad es cuando una persona obtiene, transfiere o utiliza de manera indebida datos personales de otra, usualmente para cometer fraudes o delitos.

Según el INAI, es la apropiación de la identidad de una persona para hacerse pasar por ella y asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre. La usurpación de identidad implica la obtención y uso **no autorizado e ilegal** de los datos personales.

Según la Home Office Identity Fraud Steering, del Reino Unido, es

> la recopilación de información relativa a la identidad de una persona con el fin de obtener un fraude identitario, prescindiendo del hecho que la víctima sea una persona sea una persona viva o fallecida… por lo tanto consiste en la apropiación indebida o de cualesquiera otros datos personales (fechas de nacimiento, domicilio, claves bancarias, contraseñas de acceso a redes, etc.).

El robo de identidad también se puede identificar con los siguientes conceptos: usurpación de identidad, suplantación de identidad, falsificación de identidad y de su uso indebido. Éste es el delito de mayor crecimiento en los últimos años (Jurídicas).

En general, las diferentes definiciones coinciden en que el robo de identidad es “la obtención de beneficios de cualquier índole, con el uso de los datos personales o de identidad de otro individuo sin su autorización”.

En lo que respecta a esta investigación, el robo de identidad o la usurpación de identidad es el uso de la información de identidad o datos personales de otras personas sin su autorización para la obtención de servicios financieros, como el lavado de dinero, la obtención de recursos, la venta en nombre de la persona o el robo de los recursos que estén a nombre de la persona suplantada.

1.3 Significado y alcance de los datos biométricos

Son aquellos datos que contienen la información relacionada con la morfología, mediciones o cualquier tipo de métrica o característica física de un individuo que permita su distinción única, los cuales se usan para para fines de identificación. Para ser válidos, deben ser utilizables de manera eficiente en repetidas ocasiones y que no cambien con el paso del tiempo.

Los datos biométricos deberán poder obtenerse mediante medios digitales y convertirse en formatos estandarizados y comúnmente ser utilizables y comparables mediante tecnologías que permitan su búsqueda (identificación) y comparación (autenticación) en uno u otros registros en grandes bases de datos. Uno de los pilares de la autenticación en la seguridad informática indica que, para autenticarse, se pueden usar mecanismos que distingan de manera única a la persona que reclama acceso; se denomina *lo que soy*, por lo que la autenticación biométrica podría compararse con métodos de autenticación como claves, tarjetas de identificación, *lo que tengo*, y contraseñas, *lo que sé*.

La sofisticación de las soluciones biométricas y el desarrollo de productos asociados a la obtención y explotación de esta información ha crecido en la última década y para diversos casos de usos civiles y militares (Biometric Identification Law and Ethics). Esto también ha generado grandes riesgos en la materia, ya que, al masificarse los medios de captura y el conocimiento de estas tecnologías, el robo de los datos biométricos se hace cada día un tanto más frecuente-

Esta investigación tratará de responder si, al usar de manera masiva los datos, se ha vulnerado la seguridad e identidad de los ciudadanos mexicanos o, por el contrario, se ha protegido sus derechos constitucionales de ser identificados y únicos ante el Estado mexicano.

Para el desarrollo de la investigación nos centraremos en la descripción de los datos biométricos de huellas dactilares y facial.

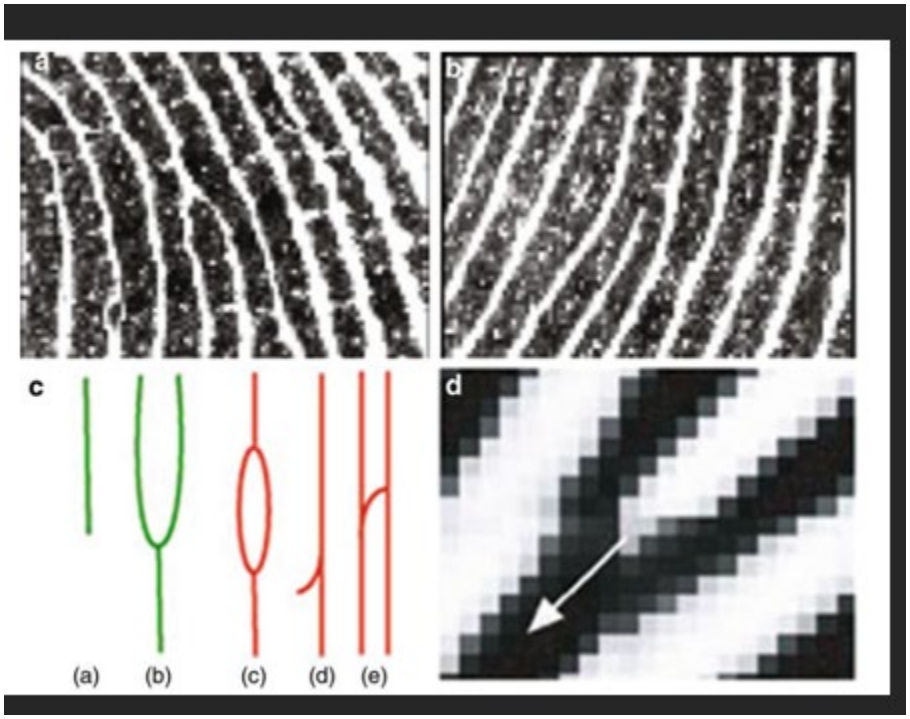
Principales características de la biometría de huellas dactilares

Las huellas dactilares se componen de crestas y valles, los cuales existen en la morfología de cada uno de nosotros. Las huellas aparecen de diferentes formas y tienen patrones, los cuales pueden ser medidos y, con estas mediciones, determinar las diferencias que las hacen únicas.

Figura 1

Clases de huellas: *a)* Arco, *b)* Tienda campaña, *c) Loop* izquierdo, *d) Loop* derecho, *e)* Espiral, *f) Loop* gemelo. Fuente: Bigun (2009).

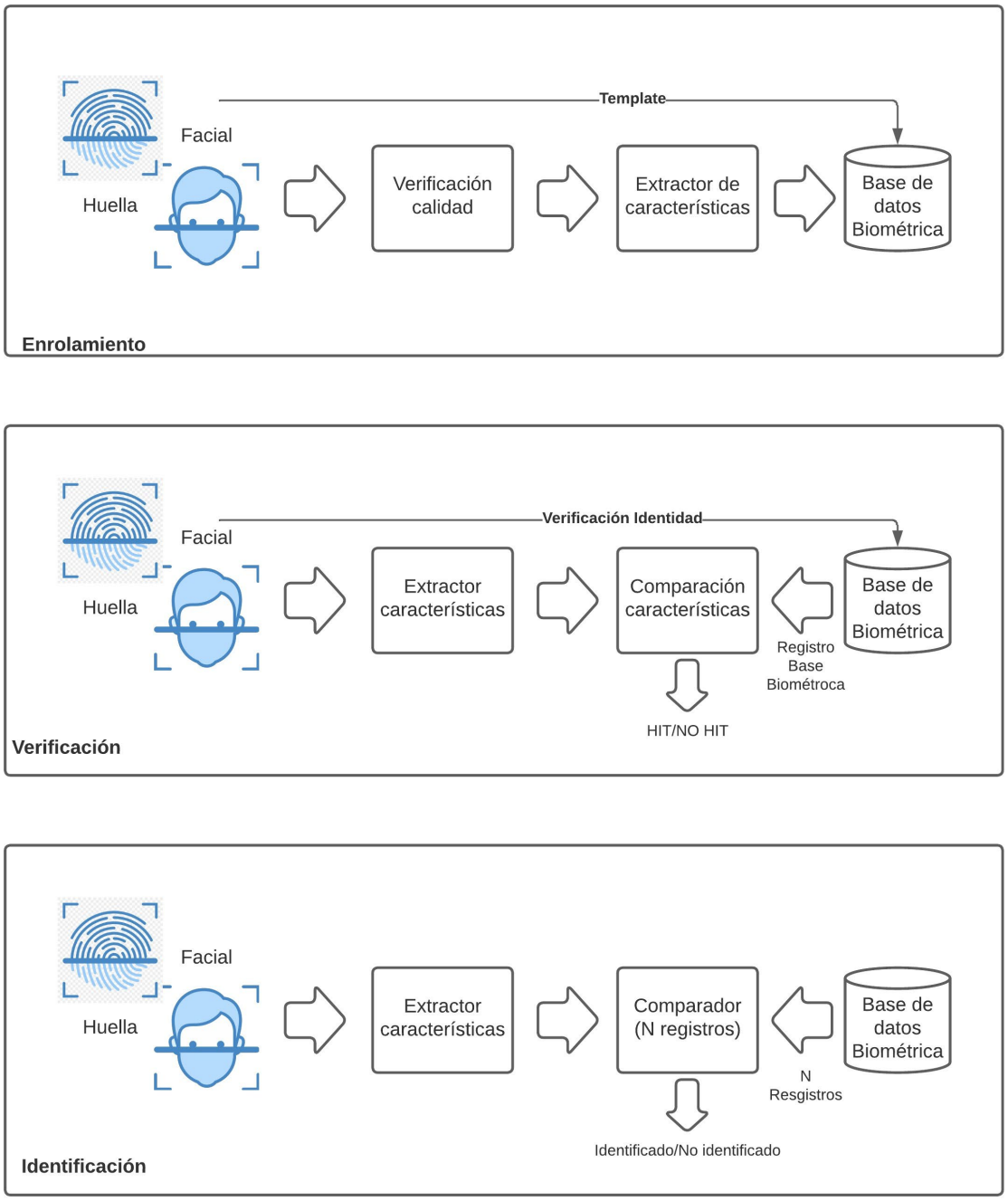
Figura 2



Ilustraciones de minucia: *a)* Bifurcaciones del valle, *b)* Viceversa, *c)* Tipos de cresta, *d)* Dirección de las minucias. Fuente: Bigun (2009).

Estas mediciones se hacen mediante dos tipos de algoritmos en la industria: los denominados *propietarios* y los *estándares*. El más popular de estos últimos es el ANSI INCITS 378-2012 o MINEX. Estos formatos permiten que, al ser almacenada la información de las huellas, se pueda reutilizar para las funciones de identificar o verificar, y la diferencia de cada formato tendrá como resultado la precisión y velocidad a la entrega de los resultados.

Figura 3



Flujos de operaciones biométrica común mente implementados. Fuente: elaboración propia.

El ciclo de vida de los sistemas de información biométrica comienza con el enrolamiento, que consiste en proporcionar los datos biométricos y compararlos con

todos los datos existentes, lo que la industria de los biométricos se conoce como identificación o búsquedas 1:N. El objetivo de esta búsqueda es que el resultado sea cero y que no existe ninguna coincidencia con algún otro registro en la base de datos biométrica. Es un sistema automatizado de identificación y comparación. En nuestro caso de estudio, el INE es el que tiene una base de datos biométrica y los ciudadanos mexicanos que cumplen 18 años son los que pueden enrolarse, y para cada enrolamiento tiene que ejecutarse esta búsqueda 1:N. Al momento de la integración de esta investigación, la base del INE tiene 98 millones de registros (únicos) de ciudadanos mexicanos que están en el padrón electoral. Esta base de datos comenzó a integrarse en 2012 y se ha mantenido a lo largo del tiempo con el registro de 10 huellas, fotografía y datos biográficos. Se puede decir que, de facto, ésta es la base de datos de identidad de los ciudadanos mexicanos, ya que hasta la fecha la cédula de identidad que debería gestionar y llevar el Renapo no cuenta con un mecanismo o base que garantice la unicidad de la identidad de los ciudadanos. Tan sólo se tiene el registro biográfico de información, sin la garantía de unicidad ya mencionada.

Hasta este momento se ha explicado que el enrolamiento es la operación que permitirá la conformación de una base de datos biométrica para poder obtener la información, obtener la mejor calidad en los patrones característicos de las huellas, fotografías y datos biográficos para almacenarlos en una base para este fin. En esta solución, también es un reto mantener la capacidad de respuesta y atención para poder validar a la persona en el momento en el que proporciona su información biométrica de dedos o facial sobre los dispositivos especializados para la toma de la información. Los procesos de enrolamiento más robustos en el mundo requieren procesos asistidos para garantizar que no existe usurpación de identidad durante el enrolamiento y que se valide la documentación que los gobiernos otorgan generalmente al nacimiento para la identificación de la identidad de cada persona, dar cumplimiento a las cartas magnas y asignar esta personalidad única.

En este proceso asistido de enrolamiento abordaremos los requerimientos que el INE ha determinado en conjunto con los órganos de control que le asisten, para poder incrementar la certeza al nivel más alto posible de la unicidad de cada

registro. Documentalmente, los datos biográficos son demostrados y tomados del acta de nacimiento. Dicho documento es el registro inicial por parte del Estado, que permite tener certeza jurídica del nacimiento de una persona y que está a cargo de las entidades federativas la ejecución del registro de población mediante los registros civiles y que están coordinados mediante el Registro Nacional de Población para garantizar este derecho. Adicionalmente, se requiere un comprobante de domicilio; éste no tiene que ver con la identidad, es un dato que se requiere para la parte electoral. La base utilizada para verificación de identidad tiene su origen en la máxima *una persona, un voto*. No nació con fines de autenticación de personas, para trámites administrativos o comerciales. Actualmente ha ampliado su uso, que es distinto a su definición original.

Finalmente, teniendo los datos generales de cada persona y su domicilio, se deben obtener las huellas e imágenes faciales de los ciudadanos.

Para la captura de huellas, se encuentra la oferta de diferentes tipos de dispositivos, los cuales cumplen con diferentes características. Una de la más importantes es la mayor capacidad de captura de dedos al mismo tiempo. Esta característica en importante en la investigación, ya que, al capturar en una misma toma la mayor cantidad de dedos, disminuye de la posibilidad de alterar su posición y, con esto, la integridad en la toma de información es precisa y confiable, y la sustitución de información biométrica no es posible al colocar en diferente orden los dedos de la mano. La morfología está asociada a la disposición del dispositivo, validando la continuidad y posición de los dedos en el patrón de morfología de la mano.

Prueba de vida: consiste en la identificación de que la huellas provienen de una mano real, del ser humano que la posee y está dispuesto a ponerla por su voluntad en el dispositivo. Varias fases de validación de diferentes elementos conforman esta prueba de vida; por ejemplo, continuidad de los dedos, numero de las falanges, impedancia eléctrica, venas, pulso o identificación de materiales, entre algunas otras que integran los dispositivos y los hace ser más sofisticados y costosos.

Característica de la imagen: resolución, profundidad de pixeles y rango dinámico mínimo. Esto permite que la imagen cumpla con los colores y la profundidad mínimos que permitan obtener las crestas y los valles, y los patrones que conforman para poder obtener las medidas con mayor definición y que se puedan distinguir unas de otras.

Capacidad de captura: captura de un dedo (*unidactilares*), de dos dedos (*bidactilares*), de cuatro dedos (4-4-2), de 10 dedos (decadactilares, en ese proceso 4-4-2). En las definiciones del *Federal Bureau of Investigation* (FBI, en español Oficina Federal de Investigaciones) y del *National Institute of Standards and Technology* (*NIST*, en español Instituto Nacional de Estándares y Tecnología), se refiere a esta capacidad con el tamaño de la platina, las características de seguridad en la captura y la calidad con las características con las que se obtiene la imagen NFIQ.

Formato: existen diferentes formatos en los cuales se almacena la información asociada a las huellas: los que están registrados por los desarrolladores de tecnología de identificación y están registrados bajo una patente se denominan *propietarios*. Éstos son los más precisos; sin embargo, su uso se limita a los que adquieren las licencias de uso o los derechos para su implementación. Son medidos por el NIST mediante la evaluación de fabricantes de Finger Print Vendor Evaluation (FPVE) 2012. Los siguientes fabricantes son los más precisos NEC, Morpho, AA Tecnology.

Adicionalmente, existen otros formatos que han cobrado una mayor popularidad por su apertura y se han vuelto estándares de facto; por ejemplo, el ANSI INCITS 378 (Generación más reciente 2012), el cual es un formato abierto de intercambio que la mayoría de los fabricantes han implementado y es el que las instituciones usan para hacer las comparaciones con las bases del Instituto Nacional Electoral.

El enrolamiento es la parte primordial de cualquier sistema de identificación. Como ya se ha descrito, da certeza de la unicidad de cada registro en las bases de datos de identidad, derivado de la búsqueda inicial de que la huella que se pretende

integrar no existe previamente y para esto se busca entre todos los registros 1:N. Se ha descrito las características ideales para la captura de información con equipos de cuatro huellas en procesos de 4-4-2 y basados en estándares de calidad altos para contar con la mayor información por cada una de las huellas posible, y tener una identificación precisa y confiable de cada registro, además del registro facial, el cual se explica con mayor detalle más adelante.

El proceso de verificación/autenticación consiste en que se compare el registro almacenado en la base de datos biométrica con el registro tomado al momento de requerir la certeza de que una persona es realmente quien dice ser y está registrado en esa base. Para este proceso, se utiliza el identificador del ciudadano asociado a su identidad del INE, el cual es el Código Identificación de Credencial CIC/OCR. El INE tiene asociada la información biométrica con este registro y se hace una comparación de la imagen facial o las huellas almacenadas con las que obtienen en el momento. Esta información es suficiente para autenticar/verificar la identidad de la persona.

La verificación es confiable al comparar las huellas de los dedos índice derecho e izquierdo y que el porcentaje de similitud sea igual o superior a 90% con cualquier huella, lo que para esquemas civiles es suficiente; sin embargo, hay que aclarar que, entre mayor sea la cantidad de minucias/características captadas de las huellas involucradas en el cotejo, se incrementa la posibilidad de un porcentaje que cumpla. Existen teorías que dicen que, de mayor información de las 10 huellas que puedan ser validada, la certeza de autenticación de un individuo se incrementa considerablemente.

El NIST tiene diferentes estudios referentes a la efectividad que tienen las soluciones biométricas y sus algoritmos. Como parte de la investigación, también se ha considerado cómo el volumen de información que se va a comparar puede aportar mayor certeza de identificación de los individuos; sin embargo, también existen documentos relacionados con los riesgos de exponer más a los individuos y se recaba la información desproporcionadamente para fines que no la requieren.

El servicio de verificación de identidad que ofrece el INE permite la comparación de las minucias de los dedos índice derecho e izquierdo, y la comparación de la imagen facial, tomados con dispositivos determinados en la regulación con la definición y profundidad establecidos, así como una prueba de vida. Dichas características son iguales a las determinadas en los dispositivos de enrolamiento. La única diferencia consiste en la capacidad de captura: de un solo dedo o hasta de cuatro en una sola toma.

Se muestra en la siguiente tabla el estándar FAP, las dimensiones y cantidad de huellas que pueden ser capturadas simultáneamente:

Tabla 1

Información de FBI y NIST sobre las dimensiones y la cantidad de huellas que se pueden capturar en cada tipo de dispositivo

Tipo	Dimensiones en cm	Huellas simultaneas
FAP 30	2.5x2	1
FAP 45	4x3.8	1-2
FAP 60	8.1x7.8	1-4

Fuente: elaboración propia.

El formato y la calidad de la huella son características que podrían depender del dispositivo o del software asociado en la verificación. No todos los dispositivos tienen la capacidad de integrar las pruebas de calidad y se valen de soluciones de software que están dentro del equipo de cómputo en el que está conectado.

En el caso de la biometría facial como medio de autenticación, el reconocimiento facial implica la comprensión de cómo se reconocen los rostros, los patrones o características particulares, como las distancias, formas geométricas o ciertas características de éste (Enciclopedia Biométrica). Ésta se refiere a otro método de autenticación utilizado en el sector financiero; se puede utilizar únicamente para casos digitales o no presenciales, ya que no ha sido plasmado para los mecanismos de autenticación presenciales. Es posible que sea una

biometría que el INE no puso en operación inicialmente en 2013 y estuvo disponible hasta 2021, cuando comenzó su operación en medio de la pandemia de covid-19. Dadas sus características no presenciales, se hace más popular.

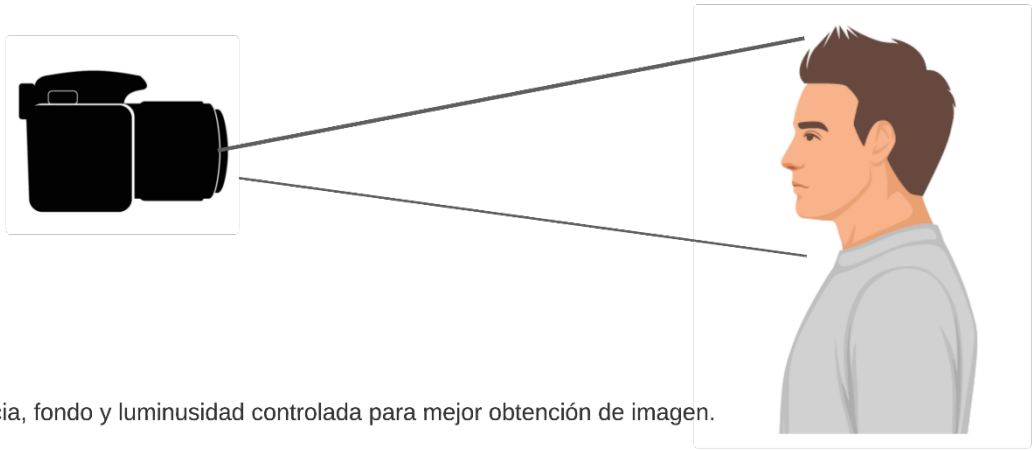
La biometría facial comienza con una fotografía digital. Ésta se toma y se alinea con respecto a la cara para establecer una posición de referencia. Las características se cuantifican para crear un mapa de contorno de los rasgos faciales que se convierte en una plantilla digital (Ricanek, 2014). En el proceso de obtener la información de las imágenes, se comparan pares de plantillas digitales y se obtiene una puntuación numérica derivado, el cual representa una medida probabilística de que son de la misma persona. Los desarrolladores del sistema establecen el umbral de similitud para una coincidencia, teniendo en cuenta un grado de tolerancia hacia los falsos positivos y negativos, con margen para que un humano tome una determinación final en un partido si es necesario (Introna y Nissenbaum, 2010).

Para el tema de las fotografías, el INE ha optado por alinearse para cumplir los requerimientos especificados por los documentos de viaje publicados por el ICAO/OACI 9303 ISO 7501: las características que se solicitan en la regulación para la toma de las fotografías faciales.

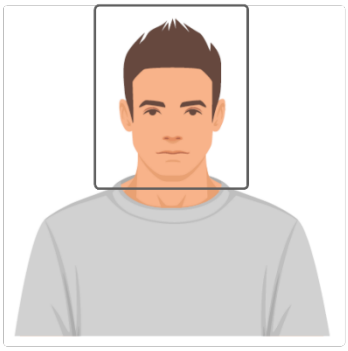
Las fotos deben ser de frente y deben presentar la menor distorsión posible, como se muestra en las siguientes imágenes:

Figura 3

Toma de imagen facial



Distancia, fondo y luminusidad controlada para mejor obtención de imagen.



Cara despejada, sin lentes y sin objetos en la cabeza.

Fuente: elaboración propia.

La fotografía debe tener una cantidad mínima de 90 pixeles, y las mejores prácticas indican que deben ser al menos 120.

En el anexo 71 de la CUB se establecen también las características de la fotografía que se tendrán en cuenta para la comparación facial, tanto para el enrolamiento como para la verificación. La CUB no precisa qué condiciones se deberían cumplir en específico si la fotografía se usa para enrolamiento o para verificación. Las características que señala son: tipo de imagen capturada,

requerimientos digitales y fotográficos, postura, expresión, iluminación, profundidad del campo, lentes, accesorios, impedimentos para la toma y bello facial.

Para el caso de las fotografías, no existen especificaciones de los equipos. Una definición y un requerimiento de los motores de comparación tienen que ver con contar con imágenes de 8mp como mínimo; sin embargo, la mayoría de las definiciones corresponde a la toma de foto, se presuponen espacios con luz y ambiente de la foto controlados en términos de uniformidad y color del fondo, así como en la distancia a la que es tomada la imagen. Pero en realidad la autenticación facial podría ocurrir en cualquier lugar y estas condiciones no siempre se cumplen. Y son los proveedores de las soluciones los que hace uso de prácticas digitales de corrección de imágenes para poder proporcionar una imagen que cumpla con las características, y que las fotos tomadas en ambientes no controlados puedan ser exitosamente comparadas con las imágenes que tiene el INE y que cumplan con las condiciones de luz, distancia y calidad de la imagen, sin distorsión, dados los controles en conjunto implementados. Por lo que el escenario de autenticación controlado o no controlado, con lo ya comentado, se puede observar que tiene ciertos aspectos de riesgo que hay que considerar.

1.4 Usos y prácticas en el uso de biométricos

Como se ha descrito, el uso de la biometría se hace para llevar a cabo la identificación plena de un ser humano basada en la cuantificación de las características de las minucias de las huellas, de las características de los rasgos faciales y cualquier otra que pueda ser medida y comparada con certeza en un futuro. Algunas de estas medidas corresponden a rasgos faciales de la nariz, las orejas, la boca o el conjunto de ellas; otras son muy importantes para el presente estudio, como son las crestas y valles de las huellas dactilares.

La certeza con la que se puede repetir la medición ha permitido que en el mundo se utilice para diferentes casos de uso, las bases más importantes conformada por el estado y que representan los casos más relevantes ya sea por el volumen de registros o por su relevancia tecnológica son los siguientes:

Gobierno de India

El gobierno de India cuenta con la UIDAI, que es la autoridad responsable de hacer cumplir la ley Aadhaar 2016 y depende del Ministerio de Electrónica y Tecnología de la información. La ley Aadhaar integra un numero aleatorio de 12 dígitos que emite la UIDAI a los residentes del país después de cumplir el proceso de verificación y este enrolamiento. La persona que desee inscribirse debe proporcionar información demográfica y biométrica mínima durante un proceso de inscripción gratuito. Este proceso se hace por única vez; después la duplicación sólo se genera un Aadhaar. Esta unicidad se logra después de la verificación de la información demográfica y biométrica 1:N.

La información demográfica requerida es: nombre, fecha de nacimiento (verificada) o edad (declarada), sexo, dirección, número de teléfono móvil (opcional) e ID de correo electrónico (opcional); en caso de inscripción basada en el presentador: nombre y número de Aadhaar del presentador; en el caso de jefe de inscripción basada en la familia: nombre, relación y número de Aadhaar del jefe de familia; en caso de inscripción de un niño: identificación de inscripción o número de Aadhaar de cualquiera de los padres, documento de prueba de relación.

Con respecto a la información biométrica, se capturan las 10 huellas dactilares, dos escaneos de iris y fotografía facial.

Se puede identificar la solución de identidad de India como la plataforma de identidad Aadhaar, con características de unicidad de los registros que están en su base de datos, autenticación, dirección financiera; y permite al gobierno llegar directamente a los residentes del país para brindarles diversos beneficios o servicios a partir del uso de un número de identificación.

Tabla 2

Información de población enrolada en India

Población total	Población enrolada	Porcentaje de población enrolada
1 372 989 959	1 277 886 750	93

Estonia

Los ciudadanos de Estonia, sin importar su lugar de residencia, tienen una identidad digital emitida por el Estado. Está basado en un sistema de identidad electrónica, el cual es llamado eID, y éste es la piedra angular del estado electrónico del país. El eID es un ecosistema de identidad que puede ser usado para cualquier cosa y forma parte de las transacciones diarias en los sectores público y privado. Las identificaciones electrónicas se usan para pagar facturas, votar en línea, firmar contratos, comprar, acceder a su información médica y mucho más.

Se usa una identificación electrónica mediante una identidad o tarjeta de identificación emitida por el estado, utilizando Mobile-ID en sus teléfonos inteligentes o la aplicación Smart-ID. Esta tarjeta está basada en la generación de protocolos de llave pública, que actualmente son los medios de firma electrónica más avanzados en la industria y en particular usan un algoritmo de curvas elípticas (ECC) de 384 bits. Es lo suficiente robusta como para que las llaves puedan perdurar durante toda la vida de un ser humano.

Tabla 3

Información de población enrolada en Estonia

Población total	Población enrolada	Porcentaje de población enrolada
1 365 884	1 352 225	99

Dada la proximidad, el estado cultural y los avances tecnológicos en América Latina, países como Colombia y Argentina cuentan también con servicios de verificación biométrica. Chile también tiene servicios similares, pero ha utilizado otra implementación tecnológica, con diferentes consideraciones y relevancia.

Colombia

En el caso de Colombia, la Registraduría Nacional del Estado Civil es la responsable de producir y administrar la base de datos de identidad de los ciudadanos colombianos. Puede ser accesible a entidades privadas autorizadas por ley para el cotejo de información biográfica y biométrica para la verificación plena de la identidad.

El acceso a la información se hace mediante instituciones terceras, las cuales son certificadas como aliados tecnológicos y mediante las cuales las entidades públicas y particulares autorizadas por la ley, podrán tener acceso al proceso de autenticación biométrica (Registraduría, s/f) .

La Registraduría en Colombia tiene disponible únicamente la autenticación biométrica dactilar y funciona mediante proveedores certificados que proveen el servicio a entidades privadas y públicas. La definición para la entrega del servicio se hace mediante el cumplimiento de una serie de requisitos que, al cumplirse, se puede proveer el servicio a estos terceros, que a su vez tienen que ser autorizados por la Registraduría.

Argentina

El SID es plataforma conectada con la base de datos del Registro Nacional de las Personas (Renaper) para validar la identidad a distancia con el reconocimiento facial de los ciudadanos argentinos.

El proceso de enrolamiento comienza al escanear el código QR del trámite iniciado, se toma una fotografía del frente y dorso del Documento Nacional de Identidad y se siguen los pasos para validar la identidad, usando la cámara frontal del dispositivo de la persona. Inicialmente fue implementado por el sector financiero y Fintech finalizó la etapa de pruebas impulsadas por la Mesa de Innovación Financiera del Banco Central (Renaper SID, s/f).

Con el SID se puede abrir una cuenta y solicitar un crédito sin tener que ir a una sucursal bancaria, entre otros servicios, facilitando así la implementación de nuevos desarrollos con más bancarización e inclusión financiera.

Capítulo 2 Como se puede implementar la biometría facial y dactilar

El uso de la biometría como medio de autenticación y ratificación de la identidad se ha sofisticado en la última década; se ha hecho particularmente popular en el uso de los dispositivos móviles en los últimos años. Sobre este incremento en su implementación, es prudente señalar que no todos los servicios biométricos que se basan en la lectura de los patrones de identificación físicos de una persona tienen la certeza y la seguridad mínimas requeridas, ya sea por la calidad en la toma o por los escenarios de comparación por el tipo de almacenamiento. Por ejemplo, esa biometría que se origina en el dispositivo móvil no es lo suficientemente fuerte como para poder autenticar a una persona para servicios bancarios y financieros, y debido a su implementación tecnológica, está basada en casos de uso simples de acceso a los dispositivos móviles, en los cuales el dispositivo se encuentra en posesión de su dueño y usuario, y el acceso físico se asume como seguro.

La biometría requiere un alto grado de certeza desde el enrolamiento hasta cada una de las verificaciones posteriores que permiten ratificar la identidad de una persona mediante la autenticación y la verificación. En México, en la Circular Única de Bancos (CUB), se han establecido estas características mínimas de captura de las huellas para conformación de las bases de datos y para uso de una única vez, las cuales han dado un marco regulatorio suficiente para la implementación de los servicios de verificación biométrica que ofrece el Instituto Nacional Electoral (INE).

2.1 Características de la autenticación/verificación biométrica solicitada en la Circular Única Bancaria (CUB)

El Instituto Nacional Electoral cuenta con una base de cerca de 98 millones de registros faciales y de 10 huellas dactilares, los cuales deben ser renovados al menos cada 10 años. Aun cuando no es su función principal autenticar a los ciudadanos para la verificación de su identidad, el propósito de la base está relacionado con el esquema electoral. E ste instituto ha definido un servicio con el cual se permite el cotejo de la información biográfica que existe en la

credencial para votar y la información biométrica, ya sea dactilar o facial, con la información que se almacena en el padrón electoral. Para tener acceso a estos servicios, se requiere hacer un convenio con el instituto, con objeto de definir el modelo de operación, la seguridad y las características de la implementación que las instituciones se comprometen a cumplir y, adicionalmente, la definición de los requisitos que se entregarán al INE para poner en operación el servicio de autenticación biométrica.

La CUB define en el capítulo segundo la integración de expedientes de crédito y datos de identificación de clientes. Los casos de uso en los cuales se debe utilizar la autenticación biométrica son los siguientes:

1. En la sección segunda – Datos de los clientes.

    a) De la identificación y realización de operaciones presenciales.

    b) Operaciones iguales y mayores a 1 500 UDIS

    c) Conformar una base de datos propia.

    d) De la identificación y contratación no presencial.

Para utilizarlo como un factor de autenticación de los usuarios y la facultad de éstos para operaciones mediante los servicios de la banca electrónica.

2. Factor de autenticación categoría 4, relativo a la información del usuario derivado de sus características físicas, tales como huellas dactilares, geometría de la mano, patrones en iris o retina, y reconocimiento facial, entre otras.

Puede también ser utilizado como autenticación para la ejecución de una transacción para la adquisición de bienes y servicios, por lo que debe considerarse la generación de una base de datos. Es importante indicar que el regulador deja un vacío, ya que en la conformación de la base de datos de huellas dactilares refiere puntualmente a la conformación asistida de la toma de las huellas mediante dispositivos físicos de cama plana; no obstante, para la verificación facial que ya se ofrece y que es permitida por el Instituto Nacional Electoral, no indica los procedimientos en los cuales podría utilizarse.

Autenticación biométrica presencial

La autenticación biométrica presencial refiere a que la persona interesada en la validación de su identidad se encuentra presencialmente en el lugar donde se le requiere demostrar su identidad. Para eso entrega su credencial para votar o muestra la información respectiva en ese momento, frente al dispositivo proporcionado por la institución que requiere de la validación de identidad. Esto ocurre en las instalaciones específicas del segundo en los equipos proporcionados por el mismo.

Antes de la captura de información biográfica o biométrica, el primer paso tiene que ver con la obtención del consentimiento del manejo de la información biográfica y biométrica entre la institución financiera y el INE. Una vez dado este consentimiento, se procede a la captura de información, y el principal dato que hay que capturar de la credencial para votar, el cual el empleado invariablemente debe validar como obligatorio, es el CIC/OCR, con el cual es posible identificar los datos biométricos que tiene el INE y son los que originalmente enrola.

Posteriormente, se transfiere la imagen de las huellas capturadas en el momento, éstas se compararan con el registro que se obtuvo al momento del enrolamiento y que se hizo una comparación 1:N con los ciudadanos que conforman el padrón electoral, con lo que se presume que este registro es único. Con los dos registros descritos, el INE compara y devuelve un resultado que va de 0 a 100 % de similitud entre ambas huellas para poder indicar si la persona es la misma que aparece en la credencial y que las huellas colocadas en el dispositivo coinciden en cierto porcentaje con las que están en el padrón. Entre más cercano a 100 sea, mayor es la certeza.

Con este resultado se autentica a la persona, se queda con un registro de la verificación en un tercero como el INE y, finalmente, se puede continuar con el trámite o servicio solicitado. La regulación requiere un mínimo de 90% de similitud como resultado de esta comparación.

Al momento de la integración de esta investigación, en la regulación no se permite la autenticación facial presencial y no existe institución financiera que la

utilice, por lo que se presume que ninguna institución ha solicitado la autorización de su uso. Lo anterior debido a los diferentes retos que podría representar su uso en ventanilla; no obstante, en el uso de autenticación facial para el escritorio y, sobre todo, para la población que ya no cuenta con una buena definición de sus huellas resulta ser una alternativa viable, funcional y segura.

Autenticación biométrica no presencial o remota

La autenticación biométrica remota es aquélla que se lleva a cabo fuera de las instalaciones de la entidad financiera, en cualquier otro lugar. Es necesario hacer una precisión relevante: aun cuando la autenticación se haga fuera de las instalaciones de la institución financiera pero frente a un empleado y con los equipos de dicha institución, ésta se considera presencial; por otro lado, aunque la autenticación se haga en las instalaciones de la institución financiera, si se usa el dispositivo del cliente o prospecto, por su propia mano, se considera remota.

La autenticación biométrica se hace desde un dispositivo del cliente, quien descarga una aplicación o hace uso los servicios web de la institución financiera. Estos servicios digitales deben contar con los mecanismos requeridos por la regulación para la toma de imágenes con calidad y que la información pueda transferirse sin poner en riesgo la integridad y confidencialidad tanto de la persona como de su información personal. A continuación, el primer paso que se debe seguir en este flujo tiene que ver con obtener el consentimiento del cliente.

La información se captura desde el dispositivo del cliente o prospecto. Se presume que el dispositivo está actualizado y no está en riesgo, que el cliente o prospecto autoriza e inicia la ejecución bajo su propio riesgo y por su voluntad en este proceso. Se continua con el consentimiento, en el cual el regulador ha puesto énfasis en la protección de los datos personales y las biometrías, dado el tipo información que se va a transportar y dados su relevancia y riesgos. Pero en el caso de los servicios móviles, la información en un principio pasa por canales de comunicación que no son propiedad ni del cliente o prospecto, ni de la entidad financiera, por lo que contar con el consentimiento para el manejo de información, sus flujos encargados y responsables es un eslabón necesario en el adecuado

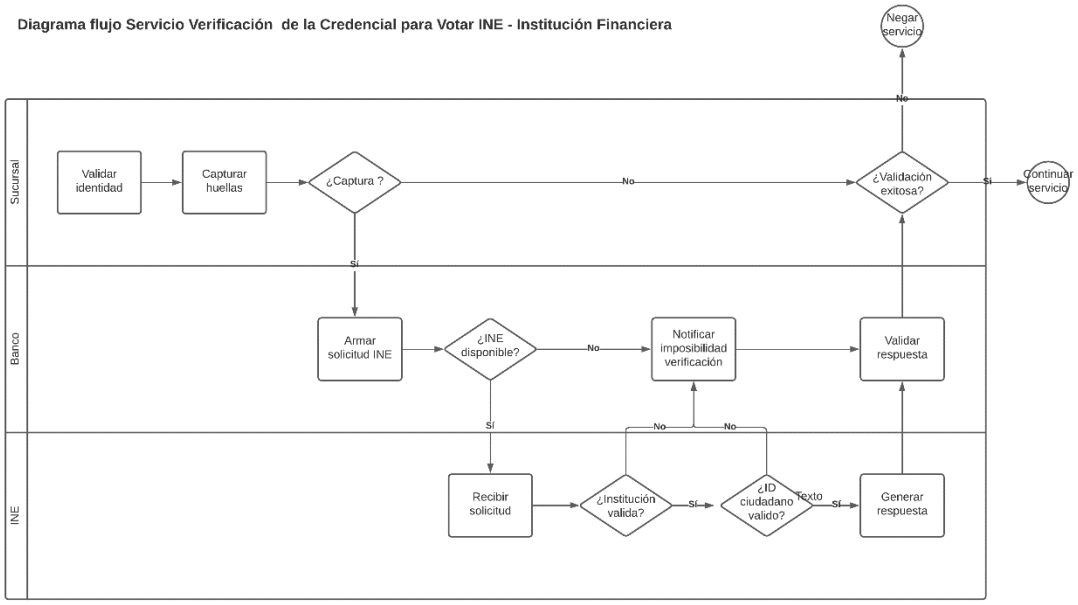
manejo de la información, su protección, validación y destrucción en caso de ser necesario.

La operación de los servicios de verificación de los datos la podemos identificar en el marco de la Ley de Protección de Datos Personarles en Posesión de Particulares y por los sujetos obligados. Ambos buscan una amplia protección a los derechos fundamentales de los individuos al cuidar su identidad y que no sea vulnerada. Dado el contexto como ya fue descrito, el uso de las aplicaciones con las que se hace la verificación biométrica es decisión exclusiva del ciudadano y él puede determinar, según esta misma regulación, si en algún momento ya no quiere compartir su información, si quiere corregirla y hacer una búsqueda exhaustiva para identificar cualquier dato relacionado. Lo anterior, de manera general, se incluye en los derechos ARCO.

Después de aceptar el tratamiento de los datos personales, según se solicita en el consentimiento y en la referencia del aviso de privacidad, el ciudadano deberá continuar con la captura inicial de la información de la credencial para votar, en la cual, como ya se ha comentado, la llave es el CIC/OCR; después se toma una fotografía denominada *selfie*, la cual es procesada para que pueda ser enviada al INE, el cual en este caso en particular obtiene la imagen que tiene en el padrón y la proporciona al proveedor tecnológico que hace la comparación en el centro de datos del instituto.

Figura 5

Diagrama Flujo Servicio de Verificación



Fuente: elaboración propia con información del INE.

En respuesta al envío de información, el INE proporciona el porcentaje de similitud que hay entre la imagen facial que está en el padrón y la que se generó en el dispositivo de los clientes o prospectos mediante las aplicaciones generadas por las instituciones financieras. Las aplicaciones que se utilicen deben ser autorizadas y validadas según las regulaciones vigentes y cumplir las especificaciones indicadas en la Circular Única de Bancos y el anexo 71 referentes.

Para ambos casos, presencial o remoto, la autenticación biométrica podría ser complementada con la búsqueda de los datos biográficos de las personas, lo que permite confirmar los tres aspectos más importantes de la identidad: datos personales, datos biométricos y quién los provee, en conjunto con la credencial para votar, son auténticos o al menos han sido verificados con la entidad de gobierno responsable al momento de establecer las identidades.

2.2 Características de la implementación de autenticación en el sector financiero

Se ha desarrollado una industria alrededor de los mecanismos de autenticación no presenciales, que consideran los requerimientos regulatorios y algunos de los elementos que integran los siguientes:

1. Lectura de información desde credencial de elector.
    a) Validación de información.
    b) Validación medidas de seguridad
    c) Integridad de información (ZLM y frente)
    d) Pantallas de validación cliente.

2. Captura de imágenes biométricas facial o de huellas dactilares.
    a) Prueba de vida.
    b) Validación de calidad de la imagen.
    c) Generación de formatos de comparación (plantillas/*templates*).

En la investigación se identificó al menos cuatro grandes escenarios para el uso de biométricos: tres para el caso de presencial y uno para el caso remoto.

En el caso presencial existen dos posibilidades dentro de las instalaciones:

1. Escritorio de tramites.
2. Ventanilla de transacciones monetarias.

Una autenticación fuera de las instalaciones pero que se hace con los equipos y personal del banco se considera presencial.

Finalmente, una última situación correspondiente al escenario remoto, el cual se inicia por iniciativa del cliente o prospecto en su propio dispositivo.

A continuación, se describe las características de implementación, espacios físicos, dispositivos y actores que permiten la adecuada operación e implementación de la solución. Como parte de esta implementación, se señalarán las diferentes medidas adicionales que podrían ayudar en la previsión de la usurpación de identidad y sus debilidades.

a) Escritorios de tramites

Los tramites en el escritorio se dan en espacios abiertos, donde el cliente o prospecto interactúa frente a frente con el ejecutivo de los servicios financieros. El cliente deberá demostrar su identidad mediante una identificación. Para el caso de la investigación, nos centraremos en los casos que comienzan cuando el cliente presenta como identificación la credencial de elector.

Al identificarse, se toman los datos biográficos de la supuesta persona que requiere el servicio y se atribuye que los datos de la credencial presentada y la persona que requiere el servicio son de ésta, y se inicia una primera interacción. Podría ser que la primera situación de riesgo ocurra en esta interacción, cuando aún no es autenticado el cliente o prospecto: podría ser que el ejecutivo ya tenga la información y suceda que en este momento se pueda dar información sensible en posesión de la entidad financiera.

Se continua en caso de requerir servicios de cuentas, los cuales pueden ser actualización de datos mismos, contratación o activación de servicios digitales, entregas de llaves o que estén relacionados con la posibilidad de ejecutar transacciones con los recursos de la cuenta, siempre y cuando los montos se encuentren dentro de los límites establecidos por la regulación.

Al concluir las transacciones, la regulación establece que se requiere autenticar o verificar mediante el uso de la verificación biométrica. En el caso particular de sucursales, únicamente se puede hacer uso de la verificación de huella. Esta verificación puede hacerse con la credencial para votar o con la base de datos que haya conformado la institución. Ambas bases están construidas con reglas que incrementan la posibilidad de que cada registro sea único.

En este momento es cuando el ejecutivo podría tener certeza de que los datos y la imagen facial corresponden a la persona que está requiriendo el servicio. Y hasta este momento se confirma con un *hit* de verificación que el porcentaje de similitud entre las huellas que están en posesión del INE y la huella que fue recabada en ese momento es superior a 90% requerido por la regulación vigente.

Existe la posibilidad de que el funcionario tenga la certeza de la identidad de la persona, pero también existe la posibilidad que el funcionario permita el uso de esquemas de usurpación o manipulación de huellas con materiales con los que intenten hacerse pasar por la identidad de otra persona. En esta situación el riesgo puede ser mitigado con los esquemas de control de acceso perimetral, videograbación o mediante mecanismos de no identificación de materiales en los dispositivos de captación de las huellas.

La regulación específica que, en la toma de las huellas, debe utilizarse sistemas que consisten en la prueba de vida. Estos esquemas buscan incrementar la probabilidad de que las huellas sean tomadas de las personas en el momento en el que se requiere y que estas tomas son directas del dedo o dedos de las personas, evitando con esto materiales que son comúnmente utilizados para la generación de huellas. Los materiales que son generalmente utilizados son látex y plásticos, sintéticos blandos, entre otros. En el caso de que la huella no identifique materiales que busquen falsificación y que la cantidad y calidad de características que hay que capturar –minucias– sea suficiente (NFIQ), se procede al procesamiento y envío para su comparación.

En el proceso del envío, el instituto ha definido un esquema que busca proteger la información de los ciudadanos y en él consta que las peticiones deben

ser protegidas mediante esquemas de criptografía. En primer lugar, los datos biográficos y las huellas son cifradas en un paquete con la llave pública del INE, lo que garantiza que esta información sólo podría ser abierta por la llave privada que el instituto posee. Posteriormente, este paquete es firmado para que el INE pueda verificar que es de una procedencia valida; es decir, de la institución que posee la llave privada y que entregó al INE su llave publica para poder verificar el envío de los paquetes con información personal. Si la firma de una institución que tiene un convenio con el INE es válida, se procede a la apertura del paquete con la llave privada y, posteriormente, con la información se busca la huella que consta en el padrón electoral y se usa para compararla con la huella que está recibiendo; adicionalmente, compara los datos biográficos. El porcentaje de similitud en la comparación de ambas huellas y el resultado falso o verdadero de los datos biográficos conforman un paquete de respuesta para las instituciones, en el que bajo ninguna circunstancia se proporcionan datos personales y sólo los resultados antes mencionados.

En esta parte del proceso al menos se permitieron tres intentos. Si no fue posible obtener y si algunos de los datos biográficos no correspondían con los que, por procedimiento, el ejecutivo la toma de la credencial o mediante los procesos automatizados de lectura de caracteres se toman directamente de la credencial.

En esta parte del proceso pueden existir diferencias en la funcionalidad de las implementaciones por cada institución y son las siguientes situaciones:

1. No es posible modificar en el sistema la información que es capturada de la credencial y se registra lo que se ha obtenido de la lectura.
2. Se permite la modificación de cierta información; sin embargo, los datos llave, como son el CIC/OCR/CURP, no permiten modificaciones.
3. Se permite la adecuación de cualquier dato. No registra control alguno, dejando sin controles la captura.

En este punto particular, se puede considerar de riesgo no tener controles y permitir que se modifique la información; sin embargo, por el contrario, muchos

clientes podrían abandonar su solicitud por no tener la certeza de que la información proporcionada es integra y el sistema funcional para su captura.

Al concluir la verificación de la información y las validaciones adicionales que las instituciones financieras deben ejecutar por regulación, se continúa con la contratación. Para fines de esta investigación, sólo nos centraremos en que se deberá conservar el consentimiento que el cliente otorgó para poder verificar la información con el INE. El consentimiento y la respuesta que el INE generó deberá formar parte del expediente con el folio correspondiente.

Es posible que, dadas las características de los dispositivos de enrolamiento 4-4-2, sólo sea en el escritorio donde se lleva a cabo esta actividad, la cual deberá ser posterior a una autenticación exitosa con el INE. No existe cambio, sino que las huellas tomadas se almacenan en la propia base de los bancos, la cual se basa en una autenticación exitosa con el INE y, posteriormente, se reutiliza en las subsecuentes operaciones que hace el banco.

En mi experiencia, sin entrar en detalles, casi ninguna institución ha formado personal calificado para atender las necesidades que requiere mantener el motor de comparación biométrica con la calidad, integridad y seguridad suficientes, por lo que podría quedar en duda si este elemento es lo suficientemente robusto en su conformación y mantenimiento, y no representa un riesgo mayor para el cliente y la institución financiera.

b) Ventanilla de transacciones monetarias

Esta funcionalidad únicamente es utilizada para la confirmación de la verificación de identidad, al presentar la credencial para votar se capturan ambos dedos índices y, con el resultado, se continua la operación solicitada. Normalmente sólo se captura el CIC/OCR. Podría ser que aquí hay un factor de riesgo, ya que la credencial misma tiene elementos de seguridad adicionales, como el año y el número de emisión, que podrían y deberían ser capturados para garantizar que la identificación no es de un usurpador al validar que corresponde plenamente a los datos con los que el banco abrió la cuenta, o que al menos existe una secuencia lógica de información que

permita dar mayor certeza de que los datos plasmados en la identificación corresponden a los que se presentan en ese momento.

Por otro lado, el tema de usurpación de identidad al usar huellas de materiales sintéticos que buscan copiar las huellas de la persona dueña de la identidad, en esto los mecanismos de identificación tienen un avance considerable, se puede detectar un gran número de materiales y se puede poner a prueba que el material colocado sobre el dispositivo corresponde a piel humana con condiciones de vida, por lo cual se incrementa considerablemente la probabilidad de que no se trata de una posible usurpación.

Los dispositivos varían de muchas formas, materiales y medidas de seguridad, pero bastaría que se hicieran las pruebas antes mencionadas y que se revise la continuidad de los dedos en relación con sus falanges, al menos para poder incrementar la certeza.

En este punto, se ha identificado que los equipos utilizados en una buena cantidad de los bancos tienen mecanismos externos al dispositivo; es decir, que se usan por separado la captura y la identificación de materiales, con lo que se requiere ahora un especialista en verificar los desarrollos correspondientes y así estar seguros de que se están tomando huellas auténticas, con tiempos de marcado, lo que no afecta el servicio. Muchas soluciones de identificación pueden afectar el servicio al ser lentas o no tener la certeza esperada. Por eso la calibración de las soluciones para que la calidad de la huella sea la más alta posible, la identificación de materiales pueda ejecutarse en un tiempo muy corto y el recorte y la verificación de cantidad de características sea la suficiente ayudan a que, si cumple con los mínimos de la industria, la posibilidad de que pueda compararse con la que tienen el INE se alta, rápida y certera.

El tramité concluye con la presentación de la huella y la respuesta del porcentaje de coincidencia. La regulación considera almacenar la información del archivo de la huella (*hash*), el consentimiento y el resultado, con lo que se podría ayudar en caso de un repudio de la transacción por parte del cliente.

c) Trámites fuera de sucursal con equipo y personal de institución

Estos trámites están más asociados a la apertura de cuentas y se hace la verificación de la biometría haciendo uso de los dispositivos del banco para facilitar y acelerar el alta.|

La situación es la misma que la que se presenta en los escritorios, sólo que el lugar puede ser cualquiera y las biometrías utilizadas para estos casos pueden ser huellas dactilares o biometría facial.

En primer lugar, el caso de las huellas es poco utilizado. Tal vez dos instituciones las han utilizado, no siempre con grandes resultados. Esto derivado de que el manejo de los dispositivos es complicado y no se puede tener certeza de la calidad de las huellas, con lo que la funcionalidad y la certeza de *hit* es baja y, por ende, la probabilidad de que los usuarios abandonen el proceso se incrementa. Al parecer las instituciones que lo han usado no tuvieron gran éxito con este proceso.

El uso de la comparación biométrica facial es el que ha tenido preferencia en estos casos, ya que se hace mediante una foto a la cara. Esta biometría es de reciente implementación y, aun cuando el proceso que el INE ha implementado es el mismo, tiene una diferencia importante: la institución financiera debe proporcionar la solución que hace la comparación y hacer el trabajo correspondiente de implementación dentro de las instalaciones del INE. Como ya se ha comentado, el INE bajo ninguna circunstancia proporciona la información, únicamente el resultado de comparación. La certeza dependerá la tecnología de la toma de la foto contra la *selfie* que se toma por el cliente con su dispositivo. La foto del INE cumple características internacionales de documentos de viaje, mientras que la *selfie* podría no tener la calidad y finalidad correspondiente de autenticación.

Las instituciones han desarrollado las aplicaciones que permiten obtener la *selfie* con las características necesarias para poder hacer la comparación; se hace mediante aplicaciones para este fin y se hacen integraciones con las soluciones del motor de comparación biométrica facial en el INE.

Hasta el momento de la investigación, el INE ha avanzado en estas soluciones con un número importante de instituciones financieras que ya las han

implementado. Esta solución ha permitido que las nuevas instituciones, denominadas Fintech, ya puedan tener acceso a mecanismos de verificación de la identidad. Anteriormente sólo podían hacerlo con huellas, lo cual no es muy funcional en los medios digitales. Sin embargo, ahora casi cualquier dispositivo permite la toma de la imagen facial y hacer la preparación de plantilla para la comparación en el INE y tener certeza en la verificación facial.

En estos casos, el riesgo está en que algún empleado, de manera malintencionada, tomara imágenes y las quisiera utilizar para autenticar. Cabe aclarar que la *selfie* también se acompaña de elementos de prueba de vida y materiales, los cuales se evitan que exista usurpación. En esta materia existe una certificación que valora, con diferentes ataques, que la solución los identifique, y no permite la utilización de la imagen para la comparación facial. Esta certificación es la ISO 30107, llamada Biometric Pressentation Attack Detection. Mientras obtenga un nivel alto la certificación, refiere niveles más complejos de ataque, con lo que se permite tener una verificación mucho más segura.

Por otro lado, siguen abiertas vulnerabilidades por parte del empleado, ya que tiene imágenes y datos que podrían ser utilizados de manera malintencionada, por lo que tendría que haber cuidado en estos casos de uso.

d) Trámites fuera de sucursal con equipo propio del cliente o prospecto

Este es el caso más seguro de todos porque la decisión depende del cliente o prospecto, desde la instalación de la aplicación, que en primera instancia es el caso de riesgo que se podría aplicar si se instalase una aplicación de dudosa procedencia; sin embargo, gracias a las tiendas de los dos proveedores de sistemas operativos, Android y IOS, este caso resulta un tanto complicado y poco probable, no obstante, sigue siendo posible que ocurra.

En los últimos tres años estas aplicaciones han proliferado y en los últimos dos han utilizado medios de verificación que comparan la imagen tomada con la del INE y los datos bibliográficos de la misma forma. El proceso es muy rápido y se hace desde la comodidad del lugar que tenga una buena señal de red para poder hacerlo con la agilidad necesaria. Los mecanismos ya mencionados para la toma de fotografía y la transmisión cuentan casi por defecto con mecanismos de criptografía que incrementan la seguridad en el intercambio de información. En este caso dependerá de tener una aplicación ágil y amigable para que los usuarios puedan verificarse.

Los riesgos que quedan en la materia son que se obtenga la imagen de alguna forma y que el momento de la toma sea suficiente. Podría sonar complicado, pero la realidad es que dispositivos muy pequeños pueden tener alcance para tomar la imagen y pasarla a la aplicación de manera indirecta; podría ser suficiente si no se cuenta con mecanismos de seguridad en las aplicaciones; sin embargo, al momento de este estudio no se identifica algún ataque que muestre que esto sea simple y con alta probabilidad de éxito. Por el contrario, la posible victima deberá participar de manera consciente, con lo que ya no es una usurpación si no se da lugar a un posible fraude.

Finalmente, los casos son cambiantes. Hoy en día se busca obtener la mayoría de los servicios ─de cualquier tipo─ de forma remota, y se cuenta con muchas formas de verificación de identidad, lo que presume hacerlos seguros. El

capítulo busca poner a consideración las situaciones más comunes, con los cuales se puede determinar los posibles casos de ataque y usurpación de identidad.

2.3 Casos en los que se usa la autenticación biométrica

La autenticación biométrica facial o de huella dactilar se utilizan para solicitar servicios bancarios de captación, integración y otros servicios monetarios que permitan la identificación plena de quien los solicita. La verificación biométrica viene a llenar un vacío de identificación de las personas. Como se ha comentado, México no cuenta como tal con un documento de identidad y supletoriamente se utiliza la credencial para votar. Sin embargo, este documento y la institución podrían no tener todas las funciones necesarias para dar el servicio y podría quedarse corto ante las necesidades actuales de verificación y vigilancia de la identidad.

Por otro lado, existe un elemento en la regulación referente a la autenticación de los servicios, el cual indica que la identificación biométrica es un mecanismo de autenticación de factor 4, que puede ser utilizado para casi cualquier tipo de transacción. La autenticación biométrica y los servicios de firma digital son lo que están en este nivel más alto y se podría asumir que eso está asociado a las características de certeza y no repudio que se tiene con este tipo de soluciones.

Las instituciones financieras hacen uso de la biometría en servicios más básicos, como la autenticación a sus mismas aplicaciones. Es importante diferenciar que esto tiene que ver con las aplicaciones de autenticación de celular facial y huella que no llegan a tener los niveles de certeza de soluciones probadas con uso de tecnología biométrica. Éstas sólo tienen patrones básicos de información, los cuales podrían ser vulnerados con facilidad.

Un resumen muy simple del uso de los servicios de biometría en cualquiera de su tipo es:

1. Contratación de servicios / cuentas.
2. Contratación de créditos
    a) Hipotecario
    b) Crédito al gasto

c) Consumo

d) Otros

3. Autenticación para el acceso de servicios o la conformación de cambios de estos.

Posiblemente, por lo reciente de los servicios de autenticación faciales, así como las integraciones y validaciones que se tienen que hacer para posteriormente, hacer la gestión con las autoridades, aún no se ha masificado el uso de los mecanismos de verificación facial como mecanismos de acceso a las aplicaciones móviles de los servicios financieros, ya que en ambos casos son procesos que pueden llevar seis meses o más, dependiendo de la complejidad de la solución y las tecnologías utilizadas.

Capítulo 3. Evaluación de resultados del robo de identidad

En el capítulo se hace el análisis del efecto que ha tenido el uso de la verificación biométrica de la identidad frente a las quejas que se han presentado. La evolución de los casos o su disminución pueden reflejar el efecto que se ha tenido para poder tomar medidas efectivas contra este delito.

Finalmente, se presentan algunas observaciones de aspectos que no son valorados y la ausencia de condiciones regulatorias que contribuyan a reportar y medir si las instituciones y sus clientes han sido afectadas, interna o externamente, por este delito de usurpación.

3.1 Reportes de robo de identidad

Como resultado de esta investigación se evalúan los resultados obtenidos en las instituciones involucradas. En primer término, el Instituto Nacional Electoral, el cual posee la información y provee el servicio; posteriormente, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), que es la institución responsable de la asesoría, protección y defensa a los usuarios de servicios financieros en relación con las instituciones financieras.

El robo o usurpación de identidad se da cuando una persona obtiene, transfiere, utiliza o se apropia de manera indebida de los datos personales de otra sin la autorización de ésta última, usualmente para cometer un fraude o delito. La identidad la constituyen los datos personales: nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y de seguridad social, financiera o médica, y cualquier otro dato que permita identificar a una persona.

En muchos casos el ladrón de identidad utiliza la información ilegalmente adquirida para contratar productos y servicios financieros a nombre de la víctima.

Como parte de la investigación, la Condusef recibe una queja según el tipo de servicio no reconocido por el cliente o ciudadano: tarjeta de crédito, tarjeta de débito o cheques. Esta queja es general y sólo el cliente, mediante la Condusef,

inicia la reclamación, debido a que no se puede indicar con certeza quién es el afectado, si el ciudadano o la institución. Para reclamar cuando un cliente no reconoce una transacción, la biometría permite tener elementos de identificación suficientes para indicar que la persona hizo una transacción y si la coincidencia con la información en posesión del INE tuvo un porcentaje que cumple con los umbrales de coincidencia para determinar que es la misma persona que requirió de la autenticación.

Con esta información que la institución se le requiere almacenar por al menos 10 años, lo que se conoce como no repudio y trazabilidad de la transacción, día, la cual consiste en hora, lugar en los que se hizo el trámite, el medio por el que fue solicitado y el resultado del cotejo de información de esta se permite integrar la información suficiente para el no repudio de la transacción que la institución tratara de demostrar al cliente. De no contar con la información, el cliente podría tener un resultado favorable de su reclamo, con lo que resulta que la persona que hizo la transacción no fue ella y, en este caso, la institución es la defraudada.

Para tener un mayor trasfondo del uso de los servicios, se presenta el número de instituciones y consultas hechas en el periodo de la investigación; posteriormente, se presentarán los reportes de usurpación de identidad hechos en el INE, como la entidad que presta el servicio y es la fuente de información presentada.

En el censo de 2020, el INEGI reporta una población de 126 014 024 personas, de las cuales 93 985 354 son mayores de 18 años (no existe dato público aproximado del rango de 15 a 19 años), mientras que, en enero de 2020, el padrón electoral tenía registrados 89 903 166 ciudadanos. La cobertura de empadronados en comparación con la población aproximada es de 96%, con lo que un porcentaje menor de la población no cuenta con su credencial para votar. Para el octubre de 2023, el padrón está constituido por 99 035 029 ciudadanos.

De esta población se tiene que considerar aquélla que esta bancarizada en las cuentas de captación:

> De acuerdo con la Encuesta Anual de Inclusión Financiera (ENIF) 2021, el porcentaje de la población que tiene o ha tenido una cuenta de captación, por grupo de edad ordenado de manera descendente, fue de 74 por ciento para personas mayores de 70 años; 70 por ciento para personas de 30 a 39 años; 66 por ciento para personas de 40 a 49 años y de 60 a 70 años; 62 por ciento para personas de 18 a 29 años; y 61 por ciento para personas de 50 a 59 años. (Inegi, 2021)

En promedio, representa 67% de la población. En términos de los retos de la verificación, el volumen de usuarios podría resultar no suficiente para poder formar una base por cada institución y afrontar los retos que conlleva la integración de una base gremial, porque aun con esto tendrían un volumen de riesgo significativo. Con el antecedente anterior, en 2013 comenzó la implementación del servicio de verificación y en 2021 la mayor parte de las instituciones financieras ya lo utilizaba mediante la lectura de las huellas en dispositivos especializados.

Con respecto al sustento legal del servicio, existe un vacío en relación con que si existe una función del INE para proporcionar la identidad del ciudadano. La Ley General de Población de 1974 no está en concordancia con la realidad actual, dada la necesidad de la identificación según procedimientos biométricos y digitales. Sin embargo, esta ley se complementa con un transitorio, el cual indica que, mientras no exista la cedula de identidad, la credencial para votar será el mecanismo de verificación de identidad. La referencia la hace a la credencial físicamente no se hace referencia a servicios biométricos y con lo que al no tener especificado de manera clara deja a la interpretación de los acuerdos de consejo del INE y las regulaciones secundarias de las instituciones financieras el alcance de estos mecanismos.

Con el contexto de la ley anterior, el INE puede hacer convenios con diferentes instituciones con la finalidad de promover la cultura democrática, por lo que los convenios promueven la actualización de la credencial con fines electorales y no de identidad. Hasta octubre de 2023, se tienen formalmente convenios para el

uso de la verificación de huellas con 81 instituciones, de las cuales las siguientes 52 se encuentran en el sector financiero:

Tabla 4

Instituciones que hace uso del servicio de verificación de huellas

Institución
ABC CAPITAL
ACTINVER
AUTOFIN
BANCA AFIRME
BANCA MIFEL
BANCO AHORRO FAMSA
BANCO AZTECA
BANCO BASE
BANCO COMPARTAMOS
BANCO DEL BAJÍO
BANCO FINTERRA
BANCO FORJADORES
BANCO INBURSA
BANCO INMOBILIARIO MEXICANO
BANCO MONEX
BANCO VE POR MAS
BANCOPPEL
BANCREA
BANJERCITO
BANKAOOL
BANORTE
BANREGIO
BANSI
BBVA BANCOMER

CAJA GONZALO VEGA
CELLPAY
CETELEM (BNP PARIBAS)
CI BANCO
CITIBANAMEX
CONSUBANCO
CREDICLUB
CREDIT SUISSE
FINAMEX
FINANCIERA BEPENSA
FINANCIERA MONTE DE PIEDAD
HSBC
INTERCAM BANCO
INVEX
MUFG BANK MÉXICO
MULTIVA
NACIONAL FINANCIERA-CETES DIRECTO
SABADELL
SANTANDER
SCOTIABANK
SICREA COMERCIAL
SOCIEDAD DE ALTERNATIVAS ECONOMICAS
TAREJETAS DE FUTURO
VECTOR CASA DE BOLSA
VIRAAL DISTRIBUIDORES
VOLKSWAGEN BANK
VOLKSWAGEN LEASING
WESTERN UNION FILIAL

Fuente: Consulta por medio Plataforma Nacional de transparencia No. 330031423003015

En 2022 comenzó la implementación de la comparación facial que, como se observa, está en proceso de maduración y expansión a los diferentes sectores. Como ya se ha comentado, la huella dactilar es la única verificación permitida presencialmente por las regulaciones vigente; no obstante, la comparación facial cubre una necesidad que se tiene en el sector para aquellas instituciones que no tienen sucursales presenciales/físicas.

El INE tiene formalmente convenios para el uso de la verificación facial con 21 instituciones, de las cuales las siguientes 20 se encuentran en el sector financiero:

Tabla 5

Instituciones que hace uso del servicio de verificación de huellas

Institución
ABC CAPITAL
ACTINVER
BANCA MIFEL
BANCO AZTECA
BANCO DEL BAJÍO
BANCREA
BANORTE
BANREGIO
BAYPORT
CITIBANAMEX
CONSUBANCO
CREDICLUB
GRUPO BURSATIL MEXICANO (GBM)
HSBC
IXE SERVICIOS
KONFIO

NU MÉXICO FINANCIERA
SCOTIABANK
SERVICIOS FINANCIEROS ALTERNATIVOS
TAREJETAS DE FUTURO

Fuente: Consulta por medio Plataforma Nacional de transparencia No. 330031423003015

De 2019 a 2023 el registro transaccional histórico ha sido el siguiente:

Tabla 6

Cantidad de verificaciones por año que hacen las instituciones

Año	**Total de Verificaciones**
2019	71,045,276
2020	130,204,509
2021	191,821,482
2022	223,855,124
2023	159,097,448

Fuente: Consulta por medio Plataforma Nacional de transparencia No. 330031423003015

En la entrada en vigor del uso obligatorio de los biométricos para la autenticación de los clientes, de 2019 a 2020 se tuvo un incremento de 83% en las peticiones que recibió el INE. Durante los siguientes años el crecimiento fue menor: entre 2020 y 2021 fue de 47% y entre 2021 y 2022 fue de 17 por ciento.

La mayor cantidad de peticiones que se ha dado durante un mes es de 21 540 271, en el mes de agosto de 2023. El promedio mensual máximo en lo que va del mismo año es de 19 887 181. El promedio mensual en 2022 fue de 18 654 594.

El INE no separa las consultas de huella dactilar de las faciales. Cada consulta se contabiliza como verificaciones por usuario o ciudadano, por lo que para fines de la investigación se tomará de igual forma la evaluación de resultados y

repercusiones en cuanto a la usurpación de identidad. Para este punto, no se debe deducir que cada consulta corresponde a una transacción. Existe un volumen alto de reintentos, los cuales pueden estar asociados a que las huellas proporcionadas no cuentan con la información suficiente, que tuvieron que repetirse o que se trató de intentos de usurpación.

Finalmente, mediante la plataforma de transparencia con número 330031423003015, se consultó al INE y al INAI si existen reportes, quejas, o procedimientos sobre alguna denuncia o procedimiento similar en los cuales algún ciudadano reportó robo o usurpación de identidad. En ambos casos dichas autoridades respondieron con la inexistencia de información. Posteriormente, se consultó al INE sobre si el ciudadano puede conocer qué instituciones financieras han hecho uso de la información que tiene el instituto; su respuesta indica inexistencia de dichos procedimientos o consultas.

Para el reporte de resultados se considera que existe un vacío en permitir al ciudadano saber quién ha consultado sus datos personales, dada la importancia de saber cuántos trámites de solicitud de credencial o, en su caso, notificar si alguien ha hecho un trámite para renovar la credencial se han hecho. En un sistema de mayor solidez de verificación de identidad, las partes deberían tener acceso a la información relevante que permita la consulta de información que proteja los intereses de cada actor contra la usurpación de identidad.

3.2 Resultados reportados por la Condusef

La Condusef, mediante el procedimiento de quejas, inicia el proceso de posible robo de identidad (mejor conocido como PORI): quejas que, asociadas a que las transacciones por las cuales se levantaron no son reconocidas por el cliente y la institución financiera indica tener información de que sí se llevó a cabo.

En este robo de identidad no es exclusiva la usurpación por el uso de biométricos. La Condusef ha integrado varios casos por los cuales se pudo presentar el delito; sin embargo, la información pública de PORI no indica los casos del uso de biométricos aun cuando la regulación vigente requiere la autenticación

biométrica, como se ha comentado para operaciones de apertura o por montos superiores a lo estipulado en el uso obligatorio de los biométricos.

Los casos que están señalados en el portal de la Condusef son:

— Robo de información (estados de cuenta o consulta de movimientos)

— Contraseña

— Correos electrónicos

— Conexión a sitios web

Estos casos están asociados a exponer la información biográfica de la víctima; se presume que el atacante tiene la suficiente información y que con ésta se podría tener acceso a las cuentas o a los mecanismos de autenticación del cliente, con lo que puede realizar una operación en nombre de la persona vulnerada. Asimismo, mediante un ataque de ingeniería social el cliente puede ser vulnerado para acceso a información suficiente que permita usurpar su identidad o en su casa, para la apertura de nuevos créditos solicitados por el tercero que usurpa.

Se tienen los siguientes datos históricos referente a las reclamaciones iniciadas por un posible robo de identidad conforme a las quejas registradas y orientadas a este protocolo. A continuación, se señalan las causas por las que se puede considerar usurpación de identidad, según lo estructura la Condusef.

Total de reclamaciones iniciadas

Tabla 7

Reportes de reclamaciones y PORI por año, del total de reportes cuántos son PORI

	Enero-diciembre			
	2019	2020	2021	2022
Total de reclamaciones iniciadas Condusef	310 200	192 345	252 170	230 698
Total de reclamaciones iniciadas en el protocolo PORI de CONDUSEF	6 575	2 383	2 849	2 325
ÍNDICE	2.1%	1.2%	1.1%	1.0%

Fuente: Condusef.

Las causas por las cuales se relaciona un robo de identidad son las siguientes:

Tabla 8

Causas por las cuales se puede hacer un reporte de identidad

CAUSAS
Crédito no reconocido en el historial crediticio
Crédito, tarjeta de crédito o cuenta otorgados sin ser solicitados ni autorizados por el usuario
El usuario, cliente o socio no reconoce haber celebrado contrato con la institución (crédito o depósito)
Disposición de efectivo en ventanilla o sucursal no reconocida por el usuario
Inconformidad con el cobro de productos o servicios no contratados por el usuario
Emisión de tarjeta de crédito sin solicitud

Fuente: Condusef

Entre 2019 y 2020 se tuvo una reducción relevante, la cual representa 63% de casos. En 2020 se inició la pandemia de covid-19 y podría haber situaciones coincidentes en la reducción a la exposición de información o la ocurrencia de los ataques o reportes. Para los años subsecuentes, el cambio en el aumento marginal no es relevante: 182 casos, un incremento del 3 por ciento.

3.3 Evaluación de los resultados

De los resultados obtenidos se puede observar que los servicios de verificación biométrica que han sido implementados por las diferentes instituciones del sector financiero han tenido amplia aceptación, y actualmente funcionan de forma presencial y no presencial (remota).

Como primera evaluación, el crecimiento de las consultas año con año permite identificar que las instituciones, encontraron valor en el uso de los servicios de verificación y han extendido su uso no sólo a los servicios.

Tabla 9

Cantidad de verificaciones en comparación con los reportes de usurpación de identidad

Año	INE		Condusef	Promedio PORI por verificación
	Promedio mensual	Total anual	Total anual	
2019	5 920 440	71 045 276	6 575	0.01%
2020	10 850 375	130 204 509	2,383	0.002%
2021	15 985 124	191 821 482	2,849	0.001%
2022	18 654 592	223 855 124	2,325	0.001%

Como resultado de la implementación, se nota una marcada reducción de los casos de usurpación reportados; sin embargo, como parte de la evaluación se tiene un punto que pudo afectar el comportamiento y no tener efecto directo en la verificación de los clientes y prospectos, quienes pudieran verificar su identidad en este periodo. Durante el tiempo sujeto a evaluación se presentó la pandemia de covid-19 y las causas de transmisión del virus eran tocar lugares infectados, por lo que esto puede afectar directamente el resultado de la investigación.

Finalmente, se debe considerar que el incremento de verificaciones de huella dactilar tiene que ver con la implementación en los diferentes casos de uso de verificación de operaciones reguladas y no reguladas. En relación con el incremento de solicitudes, se puede observar la disminución en los reportes asociados a un posible robo de identidad. Y no sólo la diminución de casos reportados en el primer

año de la implementación de esta medida regulatoria, sino en el comportamiento posterior que ha mantenido el número de reportes estables.

Habría que verificar si los casos que permanecen fueron objeto de uso de la biometría, lo que resulta complicado y que no se cuenta mayor información, ya que las entidades del gobierno responsables de proporcionar la comparación biométrica no tienen ningún registro de las incidencias que ha sufrido el padrón electoral, ya sea en la usurpación de registros que han logrado cambiar, el uso de homónimos que se registran por primera vez con datos y documentos falsificados, o cualquier otro caso que permitiera cambiar de origen la información fuente en poder con el INE.

Conclusiones

La verificación biométrica en primera instancia dactilar ha permitido sin duda la disminución de los casos de usurpación de identidad en el sector financiero en México. La disminución de los casos que se han presentado desde que la medida fue obligatoria para el sector a la fecha se mantiene estable. Permite a los usuarios de dicho sector y a las autoridades y los actores tener condiciones favorables en la verificación de identidad de los ciudadanos mexicanos. Sin embargo, los riesgos que quedan en el seguimiento y cuidado de los datos biométricos son un área de oportunidad que debe atenderse a la mayor brevedad posible.

Como se indica en las hipótesis propuestas:

Comprobación de operación

Resultado de autenticación (x_1) disminuye el Robo identidad (y_1) y los casos de robo de identidad (y_2).

Se puede observar que el resultado de la verificación biométrica ha contribuido en la reducción de los casos de robo de identidad según los reportes de la autoridad y la cantidad de consultas que se hacen al regulador. Dada mi experiencia en el sector y el aprendizaje derivado de la investigación, considero que las áreas de oportunidad que se identifican en la investigación podrían aportar en la prevención del fraude y la correcta identificación del mismo, si se aplican acciones en los siguientes actores.

a) Ciudadanos

El ciudadano, como se ha comentado, podría considerarse el eslabón más débil y se debe generar una cultura de riesgo en la cual aprenda y actúe protegiendo su información personal, sensible y no sensible. Mucho se ha documentado de internet, pero eso no basta. Tiene que ir más allá: contestar el teléfono, dar una credencial en la entrada de un edificio, simplemente confiar y no confirmar el uso adecuado de la información para cualquier operación en la que se le requiera.

Se debe vigilar al requerir y proporcionar información para continuar con el tratamiento que se le dará, procurando siempre ver más allá de la atención

inmediata, sobre la protección a largo plazo, para no incurrir en riesgos innecesarios o simplemente verificar sin entregar. Los elementos para implementar identidad soberana podrían considerarse el elemento más complejo, que permite elegir el qué, cuándo y cómo se entrega información con el reto correspondiente del control permanente de su titular, dado que las regulaciones vigentes y las leyes en materia de población; por ejemplo, las asociadas a la identidad de las personas, son obsoletas y no han sido actualizadas para la situación actual, en la que el cuidado y la soberanía de los datos de identidad se deben privilegiar y dejar en la decisión de los titulares de los datos la decisión soberana sobre qué información proporcionar, su finalidad y hasta la vigencia para su destrucción y condiciones en la que se proporciona presentas y futuras.

Sin embargo, esto aún no es posible, por lo que la conciencia en la protección y perjuicio que se puede llegar a tener por un mal uso de información personal en manos de actores malicioso puede ser catastrófico.

Como ciudadano, orientar e insistir en no dar información puede parecer una actividad menor, pero es de lo más relevante.

b) Instituciones financieras

Las instituciones financieras deberán implementar los más altos estándares de seguridad en el ciclo de vida de la información que reciben de sus clientes. Deberán almacenar sólo aquélla que es requerida por la regulación y sería óptimo que privilegiaran la soberanía del cliente en la protección de la información; es decir, que no obstante que la información de verificación de la identidad se quedará en posesión del banco, sea el mismo usuario el que tenga acceso a la misma y provea, de ser necesario, la autorización para la verificación de la misma en futuras condiciones, sin proveer acceso a empleados, mucho menos dejarla para el libre acceso interno o para otras instituciones.

Las instituciones financieras podrían integrar y formar un frente más coordinado y organizado contra el fraude. En aquellos casos en los que se presuma la usurpación de identidad o que sea confirmada, la integración de bases de datos de prevención del fraude con un elemento de protección con la conformación de

listas preventivas o de bloqueo, aportaría a contar con elementos robustos y oportunos para una identificación preventiva de los atacantes. Los elementos aislados de las instituciones no permiten integrar una base suficiente de riesgo; los elementos integrados de una base de posible usurpación o de listas negras contribuirían de manera importante a identificar aquellos casos en los que el INE pudo ser vulnerado. También una adecuada implementación de los servicios biométricos que proteja la información y no se permita el acceso abierto y sin control a los información biométrica o biográfica.

La falta de transparencia coordinada para reportar todos los incidentes y el seguimiento correspondiente, que permita más allá del riesgo reputacional incrementar y vigilar las situaciones de riesgo con el ciudadano, gobierno y en el mismo sector.

c) Gobierno

Para tener mayores y mejores elementos de protección de la identidad, es necesario avanzar en las leyes en la materia. Se han hecho y plasmado buenos esfuerzos en poder alinear a una condición vigente los elementos de identidad, los datos biométricos, la identidad digital y los datos biográficos. Aún no se tiene éxito, pero las leyes que se han propuesto en materia de identidad digital y de población son buenas y permitirían ponerse al día, estableciendo mejores condiciones en la verificación de identidad. La condición actual, con el INE sin atribución y sin elementos suficientes en la verificación de identidad, no permite evolucionar en dar el control al ciudadano de su información. Puntualmente las leyes y condiciones de identidad en México podrían considerar aspectos de vanguardia como:

1. Identidad soberana
2. Protección de información en su generación y ciclo de vida.
3. Identidad distribuida / federación.
4. Robustecimiento de ARCO, con supervisión a quien ha consultado la información.

Los elementos anteriores se pueden resumir en que el ciudadano es responsable de dar acceso a su información, determinar la finalidad de su uso, la temporalidad que da acceso y el retiro del mismo, siempre permitiendo la supervisión de quién, cómo y para qué tuvo acceso, siendo el centro de poder saber en el menor tiempo posible quien está consultando la información con la finalidad que los servicios funcionen para los ciudadanos.

El servicio de verificación de identidad que proporciona el INE es un gran paso, pero no es suficiente y no permite la adecuada estructuración para que el ciudadano realmente sea el dueño de su identidad y que cuente con todos los elementos para la protección y cuidado de esta.

Bibliografía

Agarwal, R., Jalal, A. y Arya, K (2020), A multimodal liveness detection using statistical texture features and spatial analysis. *Multimedia Tools Applications,* (79), 13621-13645.

Alamri, M. y Mahmoodi, S. (16-18 de septiembre de 2020). *Facial profiles recognition using comparative facial soft biometrics* [conferencia]. I*nternational Conference of the Biometrics Special Interest Group (BIOSIG), Darmstad, Alemania.*

Anónimo (2020). *Biometrics authentication methods*. <https://bibliotex.ipublishcentral.com/pdfreader/biometrics-authentication-methods>.

Bigun, J. (2009). Fingerprint Features en Li, S.Z., Jain, A. (eds.). *Encyclopedia of Biometrics* (pp. 465-473). Springer-

Cantoni, V., Dimov, D. y Tistarelli, M. (eds.) (2014). *Biometric authentication: First International Workshop, BIOMET 2014 Sofia, Bulgaria, June 23–24, 2014: revised selected papers*. Springer Link.

Cecoban (2021). *Identidad digital / Tus datos bajo tu control y para tu beneficio*. Cecoban. <T.ly/AU63>.

Constitución Política de los Estados Unidos Mexicanos [CPEUM], 6 de junio de 2023. <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>.

Dahan, M. y Gelb, A. (2015) *The role of identification in the post-2015 development agenda / World Bank Working Paper 2015*. World Bank. <t.ly/03QS>.

Dantcheva, A., Chen, C. y Ross, A. (23-27 de septiembre de 2012). *Can Facial Cosmetics Affect the Matching Accuracy of Face Recognition Systems?* [conferencia]. International Conference on Biometrics: Theory, Applications and Systems, Arlington, Estados Unidos.

Dawn, L., Luse, A., Mennecke, B. y Townsend, A. (2011). Adoption of Biometric Authentication System: Implications for Research and Practice in the

Deployment of End-User Security Systems. *Journal of Organizational Computing and Electronic Commerce, 21*(3), 221-245.

Gonzalez-Sosa, E., Fierrez, J., Vera-Rodriguez, R. y Alonso-Fernandez, F. (2018). Facial soft biometrics for recognition in the wild: recent works, annotation, and cots evaluation. *IEEE Transactions on Information Forensics and Security, 13*(8), 2001-2014.

European Parliament – Biometric Recognition and Behavioural Detection

t.ly/CNrZ

Hassan, M. y Shukur, Z. (2022) Device identity-based user authentication on electronic payment system for secure e-wallet apps. *Electronics, 11*(1).

_____ y Hasan, M. (2021). Enhancing multi-factor user authentication for electronic payments en Smys, S., Balas, V.E., Kamel, K.A., Lafata, P. (eds). *Inventive Computation and Information Technologies* (pp. 869-882). Springer.

ID4D (s/fa). *Partitioner's Guide*. The World Bank. <https://id4d.worldbank.org/guide/biometric-data>.

_____ (s/fb). Global ID coverage, barriers, and use by the numbers: insights from the ID4D-Findex Survey. The World Bank. <T.ly/ZMam>.

_____ (2018). *Public sector savings and revenue from identification systems.* The World Bank. <T.ly/0CvQ>.

ID2020 (s/f). *Alliance partners share the belief that identity is a human right and that individuals must have "ownership" over their own identity.* ID2020. <https://id2020.org/manifesto>.

INAI. (2016). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

_____ (2018). *Guía para el Tratamiento de Datos Biométricos*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Inegi. (2021). Encuesta Nacional de Inclusión Financiera (ENIF) 2021. *Instituto Nacional de Estadística y Geografía*. <https://www.inegi.org.mx/programas/enif/2021/>.

Instituto Nacional Electoral (2016) Acuerdo de Consejo INE/CG92/2016 (DOF, 2016)

Khattri, V. y Kumar, D.. (2019). Implementation of an additional factor for secure authentication in online transactions. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 258-273.

_____, Kumar, S. y Kumar, D. (2020) Plastic card circumvention an infirmity of authenticity and authorization. *Journal of Financial Crime, 27*(3), 959-975.

Kietzmann, J., Lee, L., McCarthy, I. y Kietzmann, T. (2020). *Deepfakes: trick or treat?* Business Horizons, 63(2), 135-146.

Lancelot, C., Popovič, A. y Oliveira, T. (2013) Determinants of end-user acceptance of biometrics: Integrating the “Big 3” of technology acceptance with privacy context. *Decision Support Systems, 56*, 103-114.

Ley General de Población [LGP]. 12 de julio de 2018. <https://www.diputados.gob.mx/LeyesBiblio/ref/lgp.htm>.

Li, D. (2015). Online security performances and information security disclosures. *Journal of Computer Information Systems, 55*(2), 20-28.

Marcel, S., Nixon, M., Fierrez, J. y Evans, N. (eds.) (2019) *Handbook of biometric anti-Spoofing* (2a ed.). Springer Link.

Meta AI (s/f). *Deepfake Detection Challenge Dataset*. Meta. <https://ai.facebook.com/datasets/dfdc/>.

Munjal, N. y Moona, R. (2009), *Secure and cost effective transaction model for financial services* [conferencia]. *2009 International Conference on Ultra Modern Telecommunications & Workshops*, San Petersburgo, Russia.

Nabalon, I, Herrera, D. y Vadillo, S. (2021). *Onboarding digital.* Banco Interamericano de Desarrollo. <http://dx.doi.org/10.18235/0003605>.

Neves, J., Tolosana, R., Vera-Rodriguez, R., Lopes, V., Proença, H. y J. Fierrez, J. (2020). GANprintR: improved fakes and evaluation of the state of the Art in face manipulation detection, *IEEE Journal of Selected Topics in Signal Processing, 14(5). 1038-1048.*

Ogbanufe, O. y Kim, D (2017). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems, 106*, 1-14.

Reid, D., Nixon, M. y Stevenage, S. (2014) Soft Biometrics; Human Identification Using Comparative Descriptions. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 36*(6), 1216-1228.

Salahshour, M., Nilashi, M. y Mohamed, H. (2018) Information technology adoption: a review of the literature and classification. *Universal Access in the Information Society,* (17), 361-390.

Sedlmeir, J., Smethurst, R., Rieger, A. y Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering,* (63), 603–613.

Tariq, S., Lee, S., Kim, H., Shin, Y. y Woo, S. (octubre de 2018), *Detecting both machine and human created fake face images in the wild* [conferencia]*,* Proceedings of the 2nd International Workshop on Multimedia Privacy and Security.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A. y Ortega-Garcia, J. (2020), Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion, 64*, 131-148.

Swaminathan, A., Wu, M. y Liu, K. (2008). Digital image forensics via intrinsic fingerprints. *IEEE Transactions Information Forensics and Security, 3*(1), 101-117.

The World Bank (2021). *The 2021 ID4D-Annual Report.* The World Bank. <https://id4d.worldbank.org/>.