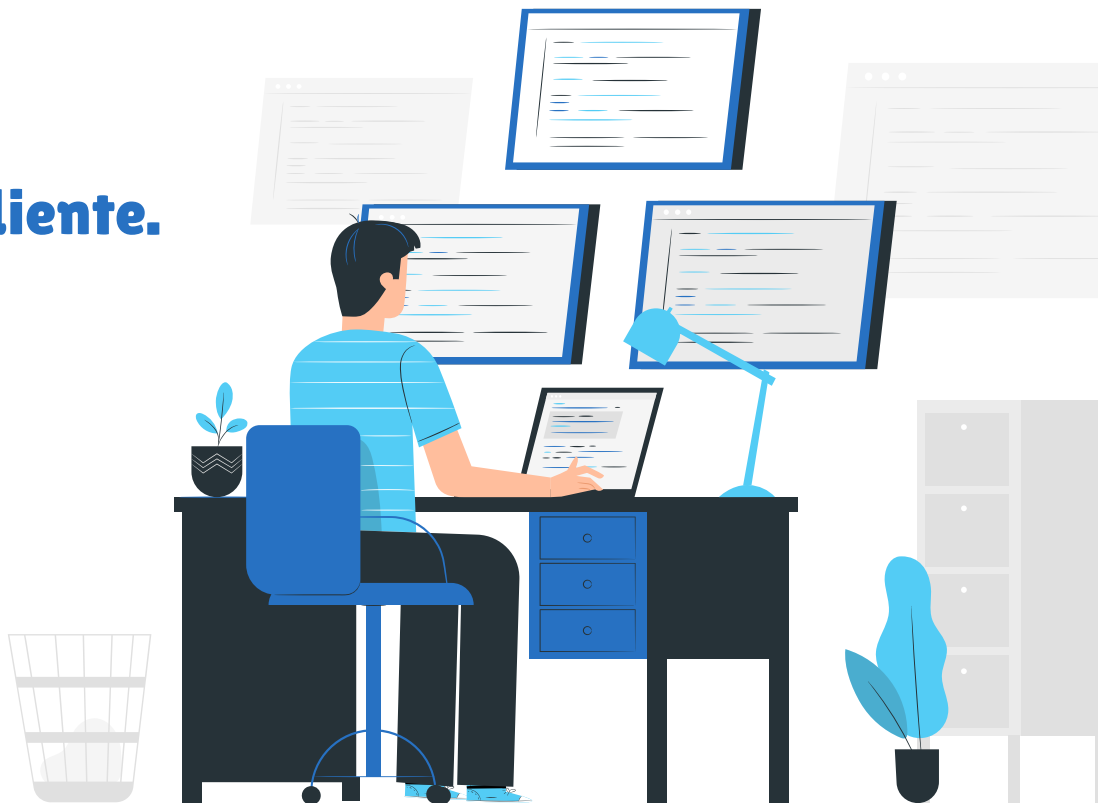


Identidad Digital: el reto pendiente.



Jonathan Garzon

Head of Digital Business & Innovation, Cecoban



¿Qué es identidad?

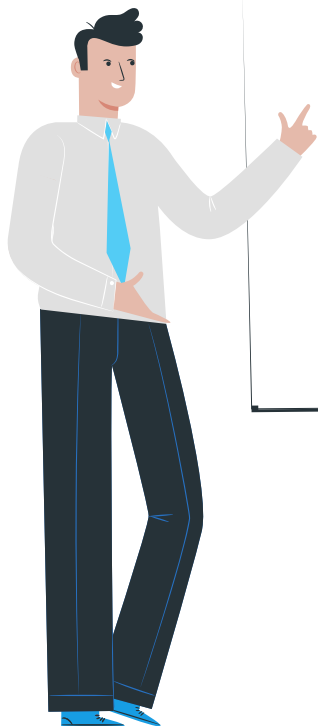
Las características de ser una persona en concreto y no otra, lo cual se determina por un **conjunto de atributos** que la **diferencian** y la vuelven **única**.

Su importancia radica en la **validación de dichos atributos** para **demostrar** que **somos** quienes **afirmamos ser**.

Cuanto más atributos haya para validar, más fuerte será la **confianza** sobre dicha identidad.



Identidad y su importancia



Términos legales:

- La identidad implica el reconocimiento del Estado de la existencia de las personas.
- En México, en 2014, se reformó el Artículo 4 de la Constitución Política, para reconocer el derecho a la identidad y al registro desde el nacimiento
- La Organización de las Naciones Unidas (ONU) estableció la meta 16.9 dentro de los Objetivos del Desarrollo Sostenible que busca garantizar para el año 2030 el derecho a la identidad para todas las personas en el mundo mediante el registro de nacimiento..

La importancia de la existencia de estos registros públicos de nacimiento radica en su función, que permite poder confirmar a terceros nuestra identidad.

Rasgo de una identidad

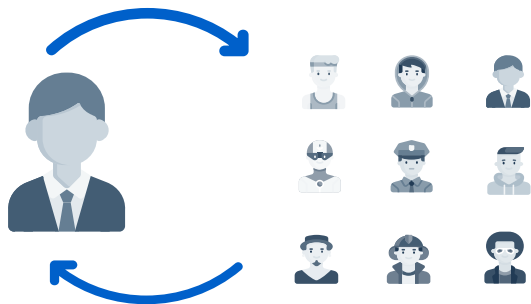
- Rasgos inherentes
 - Altura
 - Edad
 - Fecha de nacimiento
 - Biometrías
- Rasgos acumulados con el tiempo
 - Expedientes médicos
 - Preferencias
 - Comportamientos
- Datos asignados por entes públicos y/o privados
 - Teléfono
 - Email
 - No. Empleado
 - RFC
 - CURP
 - No. del pasaporte



Estos rasgos pueden ser estáticos, de poca variación, o dinámicos.

Identificación

- Proceso que permite **determinar** la **identidad** de una **persona**, generalmente en el primer o unico contacto .
- Permite tener certeza de: **¿quién es esta persona?**
- En este caso, la persona se debe diferenciar entre un gran grupo de personas (**1:N**).
- Una vez que se confíe se creará métodos para poder autenticar en el futuro



Autenticación

- Proceso de **verificación** de una **identidad previamente registrada**
- Permite tener certeza de: **¿esta persona es o no es X persona?**
- Se comparan ante un registro de datos determinado que solo confirma su similitud o diferencia (**1:1**).



Identificación



Principales factores para
lograr los dos procesos:

Autenticación



Factor de conocimiento (algo que sé): información o datos que, de forma conjunta o separada, solo una determinada persona pueda o deba saber Ej: contraseñas, claves, frases secretas.

Factor de posesión (algo que tengo o controlo): Objetos físicos (documentos, credenciales, USBs, etc.) o virtuales (correos electrónicos, cuentas de usuario, etc.) que solo una persona tiene acceso a ellos.

Factor fisiológico (algo que soy): rasgos físicos del cuerpo de una persona (Huellas dactilares, rasgos del ojo, de la cara, venas, entre otros).

Factor de conducta (algo que hago). rasgos de nuestro comportamiento que nos hacen únicos (biometría del comportamiento). Dentro de esta categoría encontramos la dinámica de la firma autógrafa, los rasgos de nuestra voz

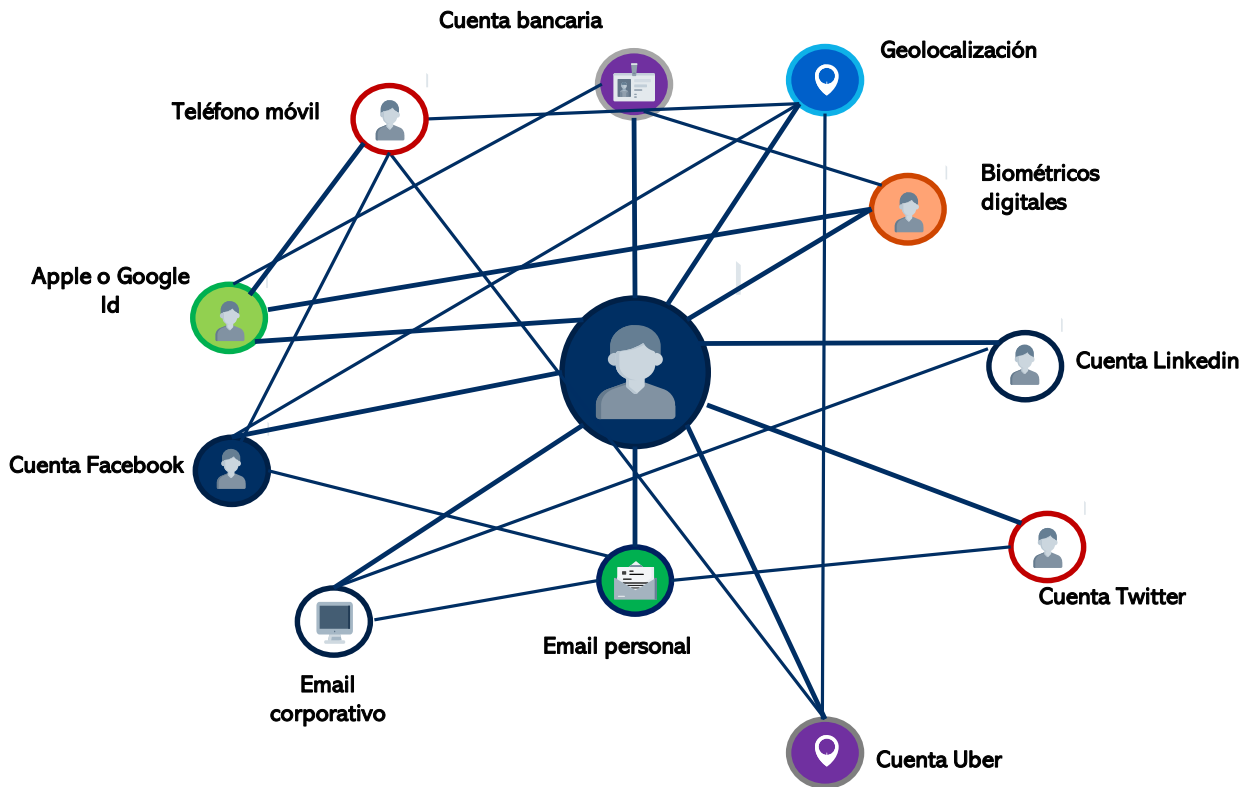
Entre más factores se utilicen en un solo proceso, se tendrá mayor certeza.

Identidad Digital



- Conjunto de rasgos característicos que permiten diferenciarnos unos de otros. Dichos rasgos viven, se procesan y se utilizan a través de la red de Internet.
- BBVA define define la identidad digital como *“el conjunto de atributos que vinculan una entidad personal con sus interacciones online”*.

Como se construye la identidad Digital



Dinámica y cambiante

Multifactorial
automatizada y poco
controlada

Las personas cambian de
hábitos, en su vida digital.

Del mundo presencial al mundo digital.

- Relaciones e interacciones + numerosas
- Totalmente a distancia, e incluso dentro de plataformas o aplicaciones fuera de nuestras fronteras.
- Esto se traduce en la necesidad de cambiar documentos de identidad físicos por métodos digitales confiables.



Ecosistema tradicional

Ecosistema digital

Generalmente se focalizan en factores de conocimiento (algo que sé) y posesión (algo que tengo).	Pueden incluir más factores combinados: fisiológicos (algo que soy) y de comportamiento (algo que hago).
Alto riesgo de falsificación de documentos físicos.	El riesgo de falsificación o robo de factores fisiológicos o de comportamiento, son más complejos por ser inherentes a cada persona.
No se delimita la entrega de información (los documentos contienen más datos que los mínimos necesarios para cada finalidad).	Se puede lograr delimitar o segmentar los datos de identidad, controlarlos y conocer con quién y para qué se usan.
Son procesos que requieren mucho tiempo y costos para su procesamiento, mientras que la experiencia del cliente es pobre.	Mejora la experiencia del cliente al hacer mucho más ágiles y sencillos los procesos de validación.
Se sobrepone la información, cada entidad genera expedientes que son posibles riesgos de robo de información.	Los datos pueden protegerse de daños, manipulación, pérdida y robo, con elementos y controles de seguridad más robustos que espacios físicos.
Requiere de infraestructura física y personal humano dedicado para llevarlo a cabo, por lo que existen limitantes de tiempo, recursos y la calidad tiene un factor de riesgo por errores humanos.	Los costos se disminuyen a escala, debido a las capacidades computacionales que actualmente pueden ser utilizadas. La calidad puede incrementarse al depender de tecnológica ya validada en procesos automatizados.
Son procesos manuales por lo que su escalabilidad es limitada.	Al ser procesos automatizados la escalabilidad es ágil, alcanzando grandes cantidades de procesos de validación de identidad o autenticación en segundos.
Se requiere mantenimiento y administración física de los expedientes para su reutilización por la misma entidad.	Se puede integrar con un mayor número de canales, dispositivos, aplicaciones, coches inteligentes, hogares inteligentes, por lo que su reutilización es casi ilimitada.
Baja reutilización externa por la alta dependencia en la confianza del personal que lo opera y los controles definidos por cada entidad.	La calidad de la información depende de sistemas electrónicos estandarizados, los cuales pueden interconectarse para ser utilizados por varias entidades.

La seguridad debe ser percibida y proporcional Combinación de factores de acuerdo al riesgo



Validación de documentos



PIN o Contraseña



Huellas dactilares



Firma autógrafa o electrónica



Fotografía digital



Iris de ojo



Análisis de Comportamiento



Smart Band – con ECG

ID y Prevención de fraudes

Problemas

Tratar a clientes como defraudadores.
Tratar a defraudadores como clientes.

Necesidad

Encontrar y detener el fraude sin frustrar a sus clientes (seguridad vs usabilidad)

Robo de identidad:

- El robo de identidad es un término incorrecto, ya que, como tal, una identidad no puede ser robada, el término adecuado debe ser usurpación o suplantación
- Y debe ser entendida como la acción cuando una persona obtiene, posee y utiliza de manera engañosa datos de alguien más, para asumir su identidad y realizar actos en su nombre.
- Ejemplo: apoderamiento y posterior uso no autorizado, de una tarjeta de crédito, una identificación oficial, así como claves o contraseñas para ingresar a sistemas, aplicaciones móviles o sitios Web de entidades públicas (SAT, INFONAVIT) y privados (banca electrónica, Uber, Facebook, WhatsApp,).



80

Lugar en términos de robo de Identidad de acuerdo con Banco de México.



Problemáticas que afectan a las víctimas

- a) **El tiempo** que transcurre entre la acción del mal uso de su identidad y el conocimiento de la víctima de los daños que esto le causó.
- b) La complejidad **de demostrar** que una persona no fue quien realizó las acciones que se le imputan.

Adicional a los perjuicios económicos, el robo de identidad puede afectar emocional o directamente en la reputación de las personas. Emocionalmente, debido a la posible **sensación que les ocasionaría el despojo** de su propia identidad y de injerencia indebida en su vida privada. En cuanto a su reputación, porque pueden **imputársele actos** de índole social que traiga como consecuencia **el rechazo** de círculos laborales, familiares, académicos o personales.



Acciones que están penadas como delitos:

Código Penal para el Distrito Federal	Artículo 211 Bis	DOF: 10-03-2014
<p>Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.</p> <p>Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.</p>		

Ley de Instituciones de Crédito	Artículo 112 Séptimus	DOF: 09-03-2018
<p>Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientas mil Unidades de Medida y Actualización, a quien utilice u obtenga, por sí o a través de interpósita persona, cualquier servicio o producto financiero proporcionado por alguno de los sujetos a que se refiere el artículo 3 de esta Ley o por una autoridad financiera o alguna de sus áreas, bajo una identidad falsa o suplantada.</p> <p>Las mismas penas se impondrán a quién para realizar alguna de las conductas a que se refiere el párrafo anterior, otorgue su consentimiento para llevar a cabo la suplantación de identidad.</p>		

Acciones que están penadas como delitos:

Ley para Regular las Instituciones de Tecnología Financiera	Artículo 131	DOF: 09-03-2018
<p>Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, a quien utilice, realice u obtenga, por sí o a través de interpósita persona, cualquier servicio, Operación o producto proporcionado por alguna de las ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos previstas en esta Ley bajo una identidad falsa o suplantada.</p>		
Código Fiscal de la Federación	Artículo 110	DOF: 01-06-2019
<p>Se impondrá sanción de tres meses a tres años de prisión, a quien: (...) VI. A quien mediante cualquier medio físico, documental, electrónico, óptico, magnético o de cualquier otra clase de tecnología, suplante la identidad, representación o personalidad de un contribuyente. VII. A quien otorgue su consentimiento para llevar a cabo la suplantación de su identidad. (...)</p>		

Datos Biométricos e identidad:



Uno de los métodos de identificación y posterior autenticación que actualmente se está utilizando es la validación biométrica, tanto **por la fuerte relación** que tiene con la unicidad de las personas, como **por lo sencillo** que puede llegar a ser en cuanto a la experiencia de validación.

No se pueden olvidar e intercambiar y su falsificación resulta de un alto grado de complejidad, aunque cabe decirlo: **no son invulnerables** y pueden generar **altos riesgos** en casos de uso abusivo, por ejemplo, la videovigilancia dirigida por reconocimiento facial.



Datos Biométricos e identidad:

Los datos biométricos los llevamos siempre con nosotros

Universales: ya que son datos con los que contamos todas las personas;

Únicos: ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas

Permanentes, ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona, y

Medibles de forma cuantitativa.

Entre los datos biométricos que refieren a características **físicas** y **fisiológicas** se encuentran la huella digital, el rostro (reconocimiento facial), etc.

Los datos biométricos que refieren a las características del **comportamiento** y los **rasgos** de la **personalidad** se encuentran la firma autógrafa, la escritura, la voz.



Identidad digital en México.

México no cuenta con un servicio electrónico abierto, ágil, sencillo y seguro para que cualquier empresa o entidad gubernamental pueda validar, no solo que ciertos datos de las personas concuerdan con sus registros o bases, sino la posibilidad de adicionar otro tipo de datos a este proceso, como los biométricos, para crear un proceso confiable de identificación.

Esto no quiere decir que no haya bases de datos biométricas en México. Existen experiencias y esfuerzos aislados (no interoperables hasta el momento) como:

- Servicio de Administración Tributaria (SAT)
- Secretaría de Relaciones Exteriores (SRE)
- Instituto Nacional Electoral (INE)
- Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR)

Aquí se almacenan algunos datos biométricos de las personas para identificar y posteriormente autenticar a las personas en sus propios procesos

Sin embargo, estos registros no pueden ser consultados por cualquier tercero en sus procesos de identidad. Existen servicios abiertos para validar datos como el CURP o los registrados ante el INE, sin embargo, únicamente son datos textuales que están plasmados en un documento, no servicios de validación biométrica.

Un buen ecosistema de validación de identidad digital permitiría a las aplicaciones y procesos tecnológicos realizar actividades con mayor precisión de la identidad de las personas, disminuyendo riesgos sobre métodos tradicionales de la identidad.



¡Muchas Gracias!

