Institución Universitaria

Modelo de administración de identidad digital (IdM) sobre blockchain para la mitigación del riesgo por suplantación en sistemas e-banking

César Augusto Tobón Betancur

Instituto Tecnológico Metropolitano
Facultad de Ingeniería
Medellín, Colombia
2020

Modelo de administración de identidad digital (IdM) sobre blockchain para la mitigación del riesgo por suplantación en sistemas e-banking

César Augusto Tobón Betancur

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director:

Mag. Javier Mauricio Durán Vásquez

Codirector:

PhD. Francisco Eugenio Lopez Giraldo

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2020

“The Internet was built without a way to know who and what you are connecting to”
Kim Cameron

Agradecimientos

A mi amada esposa Claudia y mis adorados hijos Laura y Samuel,
gracias totales por su infinito amor y paciencia.

A los gestores de este logro:
Héctor Vargas, Javier Duran y Francisco López,
sin su guía y apoyo incondicional no lo hubiera logrado,
¡Gracias amigos!

Resumen

La sociedad moderna depende cada vez más de internet para su desarrollo y normal funcionamiento, para el año 2019 se registraron más de 4.131 millones de usuarios conectados a internet en el mundo y en Colombia más de 19 millones de personas tuvieron un contrato de acceso a este servicio. Para el mismo año, internet se convirtió en el canal más utilizado a nivel transaccional en el país, desplazando a canales tradicionales como las sucursales bancarias y los cajeros automáticos. A la par con este crecimiento, se incrementaron igualmente los riesgos cibernéticos y los delitos informáticos; uno en particular es tema de constante preocupación, investigación y desarrollo para entidades gubernamentales, empresas privadas, sector financiero y universidades; el robo de credenciales y su utilización en la suplantación de identidad digital. Nos enfrentamos entonces a un reto global que es particularmente crítico para el sector financiero, el desarrollar nuevos modelos para la administración de identidades (IdM) disminuyendo el riesgo de suplantación de identidad para los usuarios finales.

La aparición de tecnologías como blockchain abre un nuevo panorama frente al problema de la identidad digital, permitiendo replantear los modelos de IdM tradicionales e incorporar fortalezas como la escalabilidad, la transparencia, la seguridad criptográfica y la inmutabilidad inherentes al sistema de bloques.

En este trabajo se investigaron y consolidaron las principales técnicas utilizadas para el robo de credenciales en la actualidad, técnicas que exponen las debilidades de los sistemas de IdM tradicionales. Al mismo tiempo se profundizó en el surgimiento de nuevos enfoques y soluciones para el manejo de la identidad digital usando la tecnología de blockchain. Gracias a esto, se llegó a la formulación de un nuevo modelo de IdM sobre blockchain denominado *IdM auto soberano con garante*, que al ser sometido a una evaluación comparativa contra los 3 modelos de IdM utilizados en la actualidad por los principales bancos del país, comprobó su menor nivel de vulnerabilidad frente a las técnicas de ataque para el robo de credenciales utilizadas por los ciberdelincuentes.

Palabras clave:

Seguridad informática, ciberseguridad, identidad digital, e-banking, robo de credenciales, blockchain.

Abstract

The modern society increasingly depends on technology and the internet for your development and normal operation. For 2019 more than 4,131 million of users were connected to the internet in the world and the same way in Colombia more than 19 million people contracted a subscription to this medium. Also, for 2019 the internet became the most used transactional channel in the country, displacing traditional channels such as bank branches and ATMs. However, along with this growth, cyber risks also increase and one becomes the concern of state entities, private companies and research sectors: the theft of credentials and their subsequent use for identity theft. We are then faced with a global challenge - that is particularly critical for the financial sector: Developing new models for identity management (IdM) by reducing the risk of identity theft for end users.

The emergence of new technologies such as blockchain, open new possibilities that allow to rethink traditional IdM models, taking advantage of features such as scalability, transparency, cryptographic security and immutability of this block system.

This work investigated and consolidated the main techniques used for credential theft today, techniques that expose the weaknesses of traditional IdM systems. At the same time, the emergence of new approaches and solutions for managing digital identity using blockchain technology was deepened. Thanks to this, a new IdM model on blockchain called self-sovereign IdM with guarantor was formulated, which, when subjected to a comparative evaluation against the 3 IdM models currently used by the main banks in the country, confirmed its lower level of vulnerability in the face of attack techniques for the theft of credentials used by cybercriminals.

Keywords:

Computer security, cybersecurity, digital identity, e-banking, credential theft, blockchain.

Contenido

Lista de figuras

Pág.

Lista de tablas

Lista de Símbolos y abreviaturas

Abreviaturas

Abreviatura	Término
ATM	Automatic Teller Machine o Cajero automático en español.
DANE	Departamento Administrativo Nacional de Estadística en Colombia.
DLT	Distributed Ledger Technology o Tecnología de libro mayor distribuido en español.
E-BANKING	Electronic banking o banca electrónica en español.
IBC	Identity Based Cryptography o Identidad basada en criptografía.
IdM	Identity Management o Administración de identidades en español.
IDV	Identity verification - Servicio utilizado para revisar que los documentos suministrados por un cliente son genuinos.
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones.
MFA	Multi Factor Authentication o multi factor de autenticación en español.
PKI	Public Key Infrastructure o infraestructura de clave pública en español.
SAAS	Software as a Service o Software como servicio en español.
WEF	World Economic Forum o Foro Económico Mundial en español.

Introducción

Entendiendo la relevancia que tiene internet en el sistema bancario del país y al mismo tiempo el riesgo de robo de identidad digital que sufren los clientes de dicho sistema, el presente trabajo partió de la siguiente hipótesis: “Un modelo teórico de administración de identidad digital (IdM) sobre blockchain podría ofrecer mayores fortalezas que los sistemas de IdM tradicionales (no blockchain), frente a la mitigación de riesgo por suplantación de identidad en sistemas de e-banking en Colombia”.

A partir de esta hipótesis se desarrolló el objetivo principal: “Proponer un modelo teórico de administración de identidad digital (IdM) sobre blockchain para e-banking en Colombia, que ofrezca una nueva alternativa frente a la mitigación de riesgo por suplantación de identidad”.

Para alcanzar dicho objetivo, fueron plateados los siguientes objetivos específicos:

- Caracterizar las principales técnicas de robo de identidad digital en internet utilizadas actualmente con propósitos de suplantación de identidad.
- Caracterizar las principales soluciones de IdM tradicionales y sobre blockchain, disponibles actualmente en el mercado, identificando las utilizadas por los 3 principales bancos en Colombia para e-banking.
- Construir un modelo teórico de IdM sobre blockchain para e-banking en Colombia.
- Comparar las fortalezas y debilidades del modelo propuesto de IdM sobre blockchain versus las soluciones de IdM actualmente utilizadas por los 3 principales bancos de Colombia, con referencia a las técnicas de robo de identidad digital.

Así pues, en este trabajo se realizó un recorrido detallado y riguroso por las diferentes técnicas utilizadas para el robo de credenciales, incluyendo el ciclo de vida que sufren éstas hasta llegar a manos de ciberdelincuentes que “juegan en las grandes ligas” del delito informático. Se realizó una revisión de diferentes modelos de IdM disponibles en el mercado y sus principales exponentes a nivel comercial, para luego profundizar en blockchain y el nuevo enfoque que ofrece al problema de la identidad digital sobre internet. Finalmente se formuló un nuevo modelo de IdM sobre blockchain que implica un cambio de paradigma y se realizó una evaluación del modelo propuesto con los modelos de IdM tradicionales que utilizan los tres principales bancos del país.

1. Marco teórico y estado del arte

1.1 Internet en la sociedad moderna

¿Cómo poder evadir el profundo impacto de internet en el mundo? – su alcance es global, su injerencia en la cotidianidad de las personas es total.

El Foro Económico Mundial - WEF - por sus siglas en inglés, es uno de los más influyentes organismos sin ánimo de lucro a nivel mundial, una iniciativa público – privada internacional que reúne más de 1.000 compañías del mundo y más de 100 países en torno al desarrollo global y los grandes retos de la sociedad moderna; de acuerdo con esta entidad, apalancados en las nuevas tecnologías y la conectividad de los sistemas informáticos, estamos viviendo la denominada *cuarta revolución industrial*, que conlleva grandes transformaciones en todos los aspectos de la vida; sin embargo y en coherencia con el uso intensivo de la tecnología, el cibercrimen se presenta como uno de los mayores obstáculos para el progreso de la humanidad y el mismo WEF pronostica pérdidas por 3 trillones de dólares para el año 2020, debido a delitos informáticos [1].

La ilustración 1 permite apreciar la relevancia de internet en el mundo y el nivel de crecimiento de los últimos años: de acuerdo con las cifras publicadas por el sitio web *Statista*, para el año 2019 teníamos 4.131 millones de usuarios [2], es decir, que tomando como base la cifra de Naciones Unidas de la población mundial en 2019 - 7.715 millones de personas [3], esto quiere decir que para el 2019, un 53% de la población del mundo contó con acceso a internet.

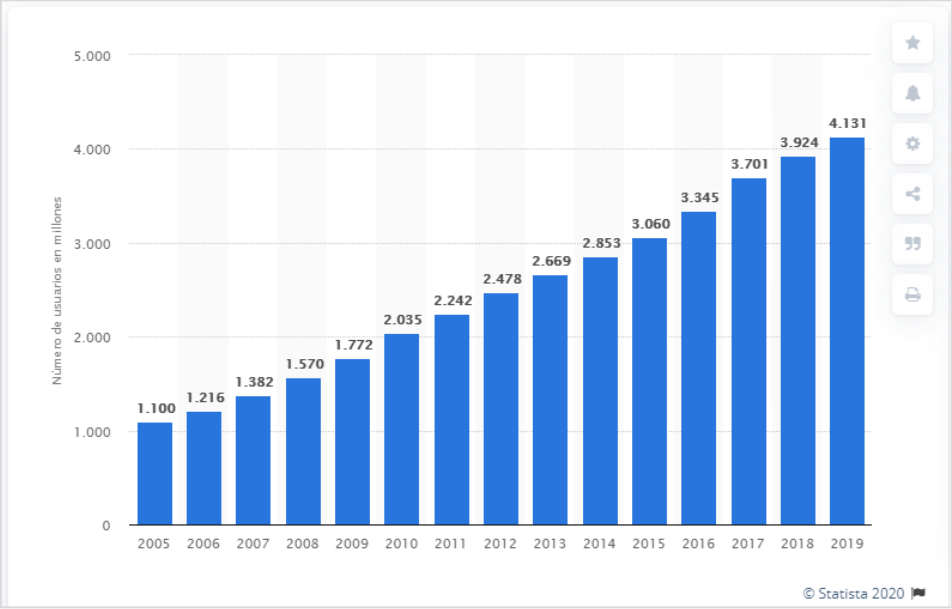

Ilustración 1 - Usuarios de internet en el mundo a 2019. Statista [2].

1.1.1 Internet en Colombia

En Colombia este crecimiento también es una realidad, de acuerdo con los datos oficiales del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para el segundo trimestre de 2019, Colombia contaba con más de 19 millones de suscriptores con acceso a internet [4] y si comparamos este número con los 48.2 millones de personas en el país - que censó el Departamento Administrativo Nacional de Estadística (DANE) en el 2018 [5] - podemos entonces decir que en Colombia el 39,4% de la población contó con acceso a internet. El nivel de acceso ha venido incrementándose en forma constante en los últimos años, como se puede apreciar en la ilustración 2.

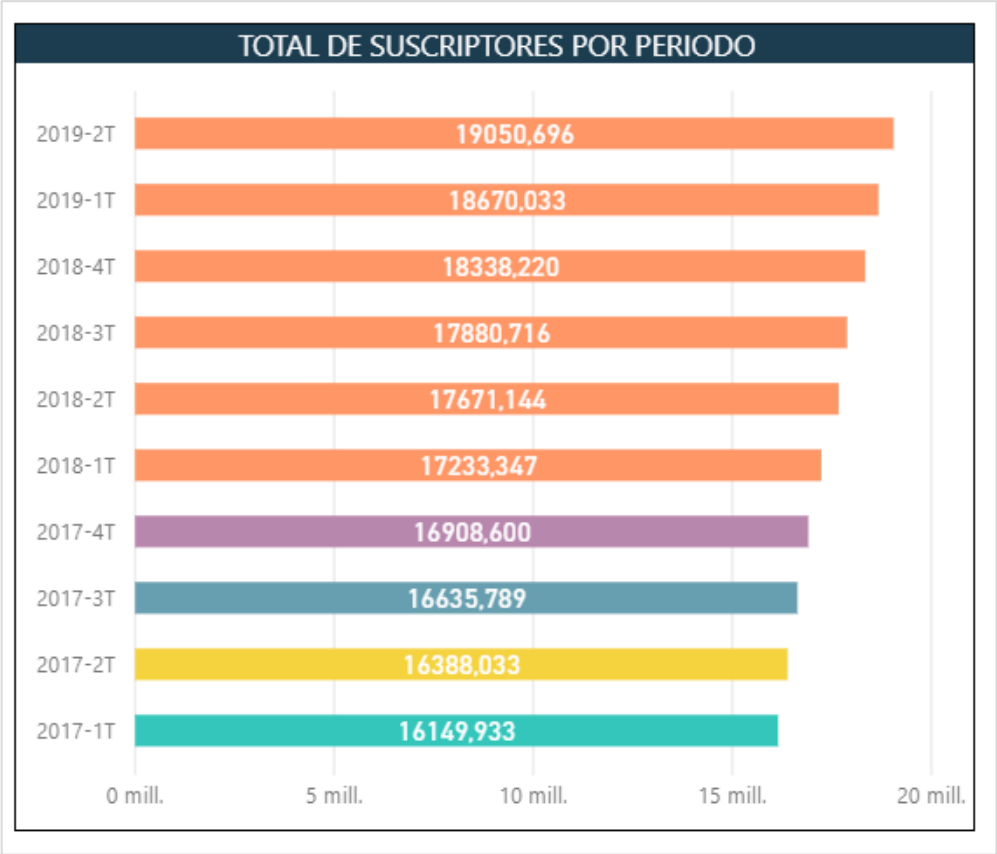

Ilustración 2 - Número total de suscriptores de internet en Colombia. MinTIC [4].

1.1.2 Relevancia de Internet en el sistema financiero colombiano

A la par con el crecimiento de suscriptores de internet en Colombia se incrementa la relevancia y el nivel de utilización de este canal por parte del sistema financiero; mirando las cifras del *Informe de Operaciones Financieras del Segundo Semestre 2019* que publica la Superintendencia Financiera de Colombia (Superfinanciera), vemos que el número total de transacciones realizadas por los bancos durante el año 2019 fue 1.678 millones de transacciones por valor de 3.3 trillones de pesos. Valores que fueron tranzados en primer lugar a través de internet, desplazando en importancia a

otros canales tradicionales como la red de oficinas y cajeros automáticos de los diferentes bancos del país [6]. Esta relevancia de internet para el sistema financiero la podemos visualizar con mayor claridad en la tabla 1 tomada de dicho informe.

OPERACIONES BANCARIAS EN COLOMBIA - 2019 — Monto en millones de pesos

Canal	Cantidad	Número total de operaciones (monetarias y no monetarias)	Monto de operaciones
Internet	0	1.678.442.853	3.383.029.739
Oficinas	6.349	535.847.213	2.899.371.421
ACH	0	121.922.813	1.251.290.348
Cajeros Automáticos	16.529	902.597.770	287.826.100
Corresponsales Bancarios	152.953	405.300.228	154.225.359
Datáfonos	580.158	753.652.234	119.803.097
Telefonía Móvil	0	3.567.658.107	92.038.203
Débito Automático	0	143.394.080	83.643.487
Audio Respuesta	0	85.401.279	1.704.325
Total		**8.194.216.577**	**$8.272.932.083**

Tabla 1 - Operaciones bancarias del país en el 2019. Superfinanciera [6].

Igualmente, en este informe podemos determinar que el 66% de las transacciones del país se concentran en 3 bancos: Bancolombia, Davivienda y BBVA. El detalle de esta distribución de transacciones por entidad bancaria lo encontramos en la tabla 2.

TRANSACCIONES BANCARIAS EN COLOMBIA POR ENTIDAD - 2019 — Monto en millones de pesos

No.	Entidad	Número de operaciones monetarias	Número de operaciones no monetarias	Número total de operaciones	Monto de operaciones
1	Bancolombia	1.445.498.646	3.330.315.977	4.775.814.623	2.715.209.787
2	Banco Davivienda	483.675.478	288.963.894	772.639.372	1.325.408.878
3	BBVA Colombia	321.539.477	302.084.379	623.623.856	713.677.970
4	Banco de Bogotá	260.905.331	384.084.230	644.989.561	1.059.719.514
5	Banco Colpatria (Scotiabank)	171.365.521	85.652.463	257.017.984	218.500.582
6	Banco AV Villas	122.344.554	76.897.611	199.242.165	124.347.148
7	Banco Caja Social	114.226.920	35.630.983	149.857.903	148.569.293
8	Banco de Occidente	109.651.359	45.512.455	155.163.814	1.005.720.893
9	Banco Agrario	83.340.148	52.819.682	136.159.830	126.834.938
10	Banco Popular	78.167.657	11.352.622	89.520.279	153.011.261
11	Tuya	48.029.945	19.796.967	67.826.912	18.958.681
12	Itaú	44.727.791	36.922.876	81.650.667	164.608.095
13	Banco GNB Sudameris	26.215.117	9.635.233	35.850.350	154.147.447
14	Banco Falabella	22.343.280	31.789.339	54.132.619	14.723.024
15	Citibank	20.323.078	1.053.547	21.376.625	214.642.628
16	Giros & Finanzas C.F.	16.397.462	883.707	17.281.169	10.853.873
17	Banco Serfinanza	14.930.333	24.990.546	39.920.879	6.514.860
18	Bancoomeva	9.922.698	1.030.117	10.952.815	17.690.131
19	Banco Mundo Mujer	7.264.818	250.991	7.515.809	4.242.999
20	Banco Pichincha	6.999.895	2.843.081	9.842.976	18.081.211
Total		**3.407.869.508**	**4.742.510.700**	**8.150.380.208**	**$8.215.463.223**

Tabla 2 - Transacciones bancarias en el país por entidad. Superfinanciera [6].

Es evidente entonces el incremento constante del número de suscriptores a internet en el país y como este crecimiento ha permitido al sector financiero consolidar internet como su principal canal

transaccional. En este punto es relevante acotar la definición del concepto de banca electrónica o "e-banking" en el contexto de las entidades financieras en Colombia.

1.1.3 e-Banking en Colombia

Se puede afirmar que NO existen una definición única del término e-banking y que éste, en realidad, es una contracción del término "electronic banking", que traducido al español sería banca electrónica.

Tomando la definición de la Encyclopedia of E-Commerce tenemos:

> "*Electronic Banking (E-Banking, Internet Banking, Virtual Banking, or Online Banking): All forms of banking services and transactions performed through electronic means. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet*." [7]. En español se puede traducir como: Banca electrónica (banca electrónica, banca por Internet, banca virtual o banca en línea): todas las formas de servicios bancarios y transacciones realizadas a través de medios electrónicos. La banca electrónica incluye los sistemas que permiten a los clientes de instituciones financieras, individuos o empresas, acceder a cuentas, realizar transacciones comerciales u obtener información sobre productos y servicios financieros a través de una red pública o privada, incluido Internet.

Cómo se puede apreciar, es una definición bastante amplia que cobija en general cualquier servicio financiero que utilice canales electrónicos, incluyendo cajeros electrónicos (ATMs), datáfonos (POST), sitios web transaccionales, aplicaciones móviles (APPs), conexiones remotas dedicadas, etc. Así pues, para el foco de estudio de este trabajo es necesario continuar acotando la definición.

Para el diario español El Economista - diario especializado en temas económicos y financieros - banca electrónica es:

> "*la prestación de servicios financieros al cliente mediante equipos informáticos de manera que pueda realizar sus transacciones bancarias en tiempo real. Tradicionalmente, este término ha sido atribuido a la banca por Internet o banca online.*" [8]

En la definición de El Economista, se encuentra una distinción importante: transacciones bancarias realizadas a través de "banca por internet" lo que permite acotar el alcance del término e-banking en operaciones desarrolladas sobre internet. Continuando con la referenciación del término, se toma la definición que ofrece Cambridge Dictionary:

> "*e-banking: The activity of managing a bank account or operating as a bank over the internet*" [9]. En español se puede traducir como: banca electrónica: la actividad de administrar una cuenta bancaria u operar como banco a través de Internet.

Así, al cotejar la definición de Cambridge Dictionary y la definición de El Economista, se encuentra un punto común en el término e-banking vinculándolo con las operaciones ocurridas directamente sobre internet.

Finalmente, para poner el término e-banking en el contexto del sector financiero colombiano, se utilizó la clasificación de canales transaccionales que reglamentó la Superfinanciera a través de la Circular Externa 050 del 2016 – anexo F0000-141 formato 444, en la que se definen 12 canales transaccionales para los bancos en Colombia, siendo uno de ellos el canal "09 -INTERNET", tal y como se puede observar en la tabla 3.

CANALES DE DISTRIBUCIÓN DISPUESTOS POR LAS ENTIDADES VIGILADAS (Circular Externa 050 de 2016 Superfinanciera de Colombia)		
01 – OFICINAS	05 – POS - PROPIOS	09 – INTERNET
02 – CAJEROS PROPIOS	06 – POS NO PROPIOS	10 – TELEFONÍA MÓVIL
03 – CAJEROS NO PROPIOS	07 – POS ADMINISTRADOS	11 – CANAL ACH
04 – CAJEROS ADMINISTRADOS	08 – AUDIORESPUESTA (IVR):	12 – PAGOS AUTOMÁTICOS

Tabla 3 – Canales transaccionales de bancos de Colombia. Superfinanciera [10].

A continuación se extrae del anexo "F0000-141 formato 444.doc" la definición que hace la misma Superfinanciera sobre el canal "09 – INTERNET" [10]:

> "*…las transacciones y operaciones de consultas de saldo realizadas por sus clientes a través de Internet y que son efectuadas directamente por medio del portal de la entidad reportante.*".

Tomando entonces las definiciones anteriores y considerando la definición de la Superfinanciera para Colombia; para el foco de estudio del presente trabajo se define e-banking como: El portal transaccional a través de internet que ofrecen los bancos y que sus clientes acceden utilizando un computador.

1.2 El cibercrimen un problema global

"Como el mundo está cada vez más interconectado, todos comparten la responsabilidad de asegurar el ciberespacio" Newton Lee

De acuerdo con el World Economic Forum, nos encontramos en *la cuarta revolución industrial,* una época de increíble transformación y dependencia de la tecnología; en la que se genera bienestar y cambios positivos en muchos aspectos de la sociedad, beneficiando a una inmensa mayoría y transformando el planeta entero [11]; sin embargo, a la par con esta transformación, este organismo considera al cibercrimen como el mayor obstáculo para el progreso de la humanidad, pronosticando para el año 2020 pérdidas del orden de los 3 trillones de dólares debido a delitos informáticos [1]. De hecho, en los pronósticos anuales del World Economic Forum, se observa que el riesgo de ciberataques ha estado permanentemente en el top 5 de los principales riesgos de la humanidad [12].

Las cifras anuales publicadas por el Internet Crime Complaint Center del FBI (IC3) son igualmente reveladoras a cerca del problema de cibercrimen en el mundo, mostrando pérdidas asociadas con

delitos informáticos por valor de 2.7 billones de dólares en el año 2018 y 3.5 billones de dólares en el año 2019 y alcanzando un impacto económico del orden de los 10.2 billones de dólares durante los 5 años de registros que lleva el IC3. Aún más relevante, es que la primera causa raíz de estas pérdidas está directamente vinculada con el robo de identidad digital [13]. En la ilustración 3, se puede apreciar el incremento constante de pérdidas económicas y el aumento del número de casos relacionados con el delito informático en los EUA en los últimos 5 años.

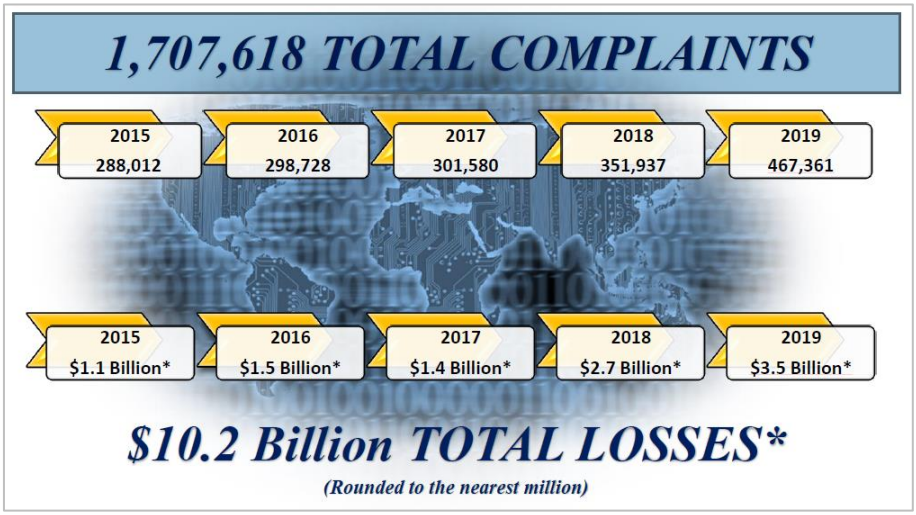

Ilustración 3 – Reporte de pérdidas por delitos informáticos en EUA. IC3-FBI [13].

1.2.1 Delitos informáticos en Colombia

En Colombia la situación no es muy diferente al resto del mundo, en el año 2009 fue aprobada la ley 1273 (conocida como Ley de delitos informáticos) en la que se legisla sobre los nuevos tipos penales vinculados a delitos informáticos y en particular el artículo 269F - VIOLACIÓN DE DATOS PERSONALES, en el que se tipifica la suplantación de identidad como "El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales" [14].

De acuerdo con las cifras oficiales del Centro Cibernético de la Policía Nacional, en lo corrido del año 2018 se recibieron 11.524 denuncias por delitos informáticos en el país (3.434 casos más que en el 2017) y entre 2016 y el 2018 el cibercrimen tuvo un incremento del 28.3%, siendo la suplantación de identidad una de las principales formas de delito informático en el país [15].

Para el año 2019, la Policía Nacional recibió 28.827 reportes de delitos informáticos - un incremento del 250% comparado con el año 2018 - y sin sorpresa, se observa como los delitos relacionadas con el robo de identidad digital continúan siendo los que más afectan a los colombianos [16]. Igualmente vemos en la ilustración 4, como los incidentes más reportados están todas asociados al robo de identidad.

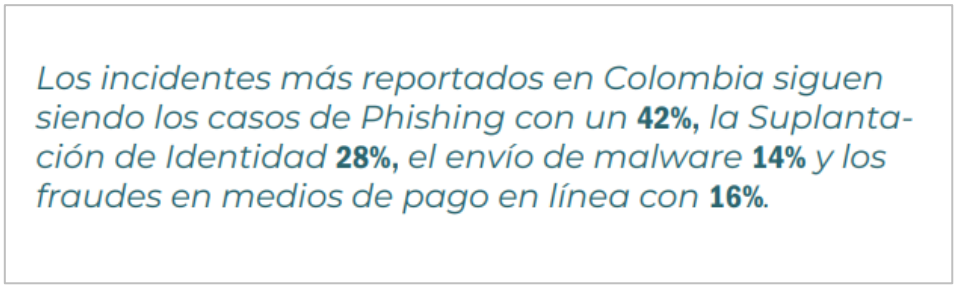

Ilustración 4 – Modalidades de delitos reportados en Colombia. Policía Nacional [14]

1.2.2 El cibercrimen y el negocio del robo de credenciales

Entendiendo el crecimiento constante de internet en el mundo, la gran relevancia que tiene para los diferentes sectores económicos y sociales en el desarrollo de servicios a través de la web y el foco natural de ataques que son este tipo de servicios, podemos afirmar que el cibercrimen y en particular el robo de credenciales es una debilidad global crítica para todo el ecosistema digital.

Existe una "industria" altamente especializada y sumamente lucrativa que se dedica al robo de credenciales y a ofrecer servicios a grandes mafias delincuenciales que operan en el bajo mundo de internet. En el año 2017 Kurt Thomas, Frank Li y otro grupo de investigadores de Google y la Universidad de California realizaron una investigación sobre la obtención y comercialización de credenciales robadas en la "darkweb", encontrando más de 1.9 billones de credenciales robadas y comercializadas a nivel global a través de foros de hackers y sitios web clandestinos [17].

Verizon - una de las compañía dedicada a tecnología de seguridad más grandes del mundo, con presencia e investigación en más de 150 países - cada año genera un informe especializado sobre las brechas de seguridad en las empresas llamado "*Data breach investigations report*" en el informe del año 2019 clasifican el robo de credenciales a través del Phishing y la suplantación de la identidad digital a través de credenciales robadas como dos de las principales causas generadoras de brechas de seguridad a nivel global [18].

De acuerdo con FBI-IC3 los casos de robo de datos, phishing, vishing y smishing fueron la modalidad base para la materialización de delitos informáticos en los Estados Unidos en el 2019 [13]. Esto ratifica el auge creciente que viene teniendo el robo de credenciales y que le suministra a los ciberdelincuentes una base para luego materializar fraudes económicos y otros delitos informáticos. De acuerdo con Symantec en su más reciente informe "*Symantec Internet Security Threat Report 2019"*, existe un activo mercado negro de credenciales en el cual se pagan desde 25 USD. hasta 5.000 USD. por credenciales robadas [19], demostrando una vez más la existencia y alta demanda de un mercado negro de credenciales robadas.

1.2.3 Del robo de credenciales a la suplantación de identidad

Ahora bien, no está de más aclarar la conexión que existe entre el robo de credenciales y la suplantación de identidad, que para algunos puede ser obvia, pero para otros se presta a confusión: el robo de credenciales es el acto de apropiarse sin autorización de las credenciales de una persona (o dispositivo), pero este acto no implica un daño o detrimento patrimonial en sí mismo, es cuando se utilizan estas credenciales robadas para suplantar la identidad digital del dueño de las mismas y cometer el fraude, alterar información o afectar la configuración de un sistema, generando en ese punto el daño o detrimento patrimonial. Vale la pena detenerse en el estudio realizado por la empresa Bluelive sobre el robo de credenciales en internet - denominado "*The credential theft ecosystem*" - en el que se describe en forma detallada el ciclo completo que usan los ciberdelincuentes para obtener, validar, depurar y posteriormente vender las credenciales robadas [20], tal y como se muestra en la ilustración 5.

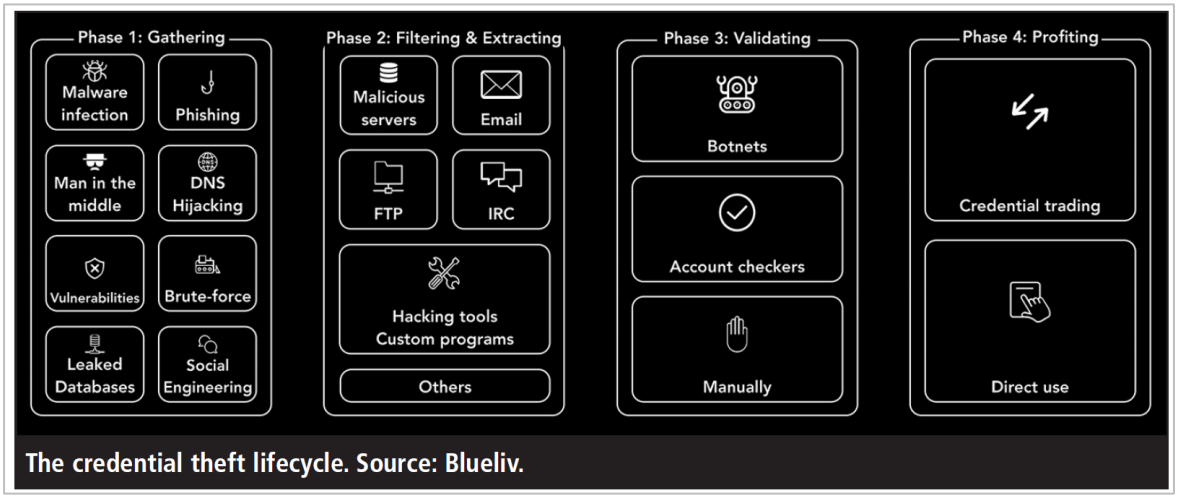

Ilustración 5 – Ciclo de robo de credenciales. Bluelive [20]

Durante la fase de *obtención de credenciales* los ciberdelincuentes utilizan diferentes técnicas para el robo de credenciales, pasando desde la ingeniería social, hasta técnicas más elaboradas como el malware especializado en el robo de credenciales conocido como "Stealers". Siendo una empresa criminal altamente especializada, los delincuentes obtienen altos volúmenes de información y por ello requieren entonces realizar una fase de *Filtrado y extracción* en la cual se clasifican, estandarizan y se organizan los datos como usuarios, contraseñas, correos electrónicos, números de identidad, direcciones físicas, etc. y se envían a los servidores centrales en los cuales se consolidan en grandes bases de datos o archivos de Excel. Luego estos grandes archivos son verificados en la fase tres: *Validación,* de forma que los delincuentes comprueban cuales credenciales funcionan y cuáles no (aún sin materializar fraude o daño). Una vez consolidado los grandes paquetes con miles o cientos de miles de credenciales ya verificadas, pasan a la fase final *Aprovechamiento;* muchas veces estas bases de datos son compradas por otros ciberdelincuentes que las aprovechan para hacer grandes fraudes o realizar otro tipo de delitos y daño informático a través de la suplantación de las identidades digitales obtenidas en la fase 1 [20].

1.2.4 Técnicas asociadas con el robo de credenciales

Es importante comenzar este apartado aclarando que no existe un referente único sobre técnicas de ataque utilizadas para el robo de credenciales y muchas de las técnicas de ataques informáticos pueden ser utilizadas para diferentes propósitos que van desde bloquear un sistema, cambiar configuraciones, alterar datos, robar información u otros. En este trabajo se recopila la información de múltiples expertos y referentes en seguridad informática que permitieron consolidar las principales técnicas de ataque asociadas con el robo de credenciales y por ende con la posterior suplantación de identidad.

El Instituto Nacional de Ciberseguridad (INCIBE) - entidad oficial del gobierno español enfocada en el estudio, normalización y creación de directrices de ciberseguridad para España y Europa - publica la "*Guía Nacional de Notificación y Gestión de Ciberincidentes*" y en ella, una clasificación de los tipos de ataques usados por los ciberdelincuentes y las consecuencias que sufren las víctimas de estos ataques. En esta guía se enumeran tipos de ataques agrupados en 10 grandes categorías [21].

Un segundo punto de referencia se encuentra en el artículo "*Understanding the credential theft lifecycle*" de José Miguel Esparza, en el que se describe a profundidad el problema del robo de identidad en el mundo y la industrialización de este tipo de cibercrimen. Así mismo, encontramos una clasificación de las diferentes técnicas usadas por los delincuentes para apropiarse de las credenciales, que el autor agrupa en siete categorías iniciales y 18 técnicas específicas [22]. En la ilustración 6 se puede observar la clasificación de técnicas propuesta por José Miguel Esparza.

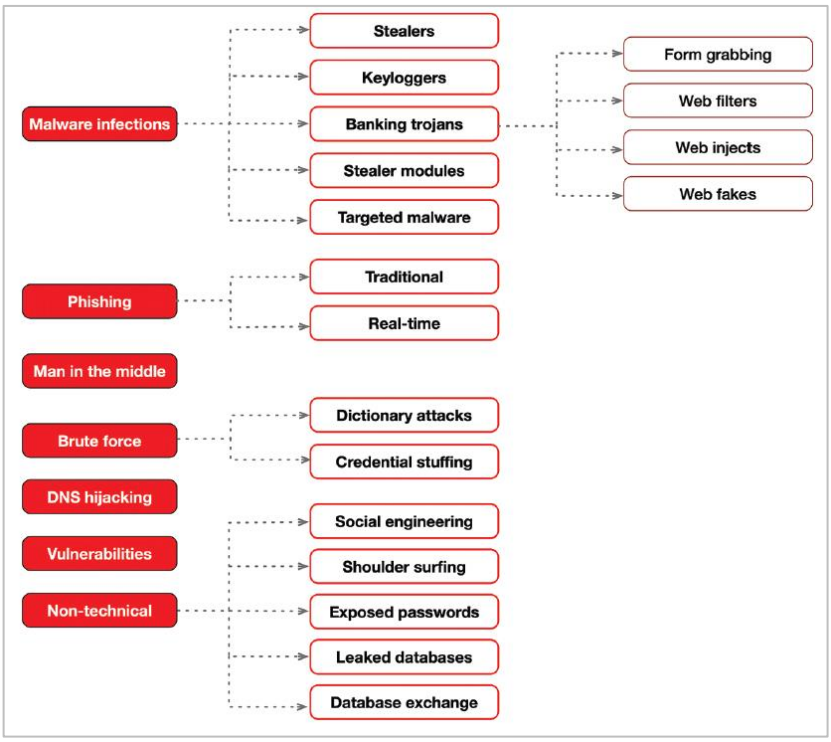

Ilustración 6 – Técnicas usados para el robo de credenciales. Esparza [22]

Otro punto significativo de referencia fue tomado del trabajo "*Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials*" en el cual los investigadores diseñaron y corrieron un programa de computadora para rastrear durante un año completo el mercado negro de credenciales robadas en el mundo e identificaron ocho técnicas de robo de credenciales usadas por los delincuentes durante la fase de obtención de credenciales [17] que se muestran en la tabla 4, junto con la cantidad de credenciales robadas fruto de cada una de estas técnicas.

Robo de credenciales en el mercado negro	
Credential leaks	3.785
Phishing kits	10.037
Keyloggers	15.579
Credential leak victims	1.922.609.265
Phishing kit victims	3.779.664
Keylogger victims	2.992
Phishing victim reports	12.449.036
Keylogger victim reports	788.606

Tabla 4 – Credenciales robadas y las técnicas utilizadas para obtenerlas. Thomas [17]

Pasando al mundo comercial, él gigante de los sistemas operativos Microsoft también ha explorado el problema de la seguridad y el robo de la identidad digital; en el artículo "*Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft*" Microsoft explora los diferentes tipos de ataques que pueden utilizarse para robar credenciales contra su servicio de directorio activo o servicios de autenticación similares, explicando igualmente algunas de las principales medidas de prevención y fortalecimiento que los administradores de dichos sistemas pueden configurar [23]. En dicho artículo se identifica un grupo concreto de técnicas de ataque mostradas en la tabla 5.

Robo de credenciales en Active Directory
Pass-the-hash attack (PtH)
Keystroke loggers
Stored passwords
Brute force attacks
Man-in-the-middle attacks
Local Security Authority Subsystem (LSASS)
Remote Keyboard/Video/Mouse (KVM)
Kerberos Pass the Ticket attacks

Tabla 5 – Tipos de ataque usados para el robo de credenciales. Microsoft [23]

A lo largo de la última década, el MITRE ha consolidado a nivel de industria, su modelo para la evaluación y ponderación cuantitativa de las vulnerabilidades tecnológicas, perfeccionando el modelo denominado *CVE - Common Vulnerabilities and Exposures*. Este modelo permite asociar a cada vulnerabilidad conocida a un código único, una descripción completa de la misma y un nivel de riesgo específico y cuantitativo que se mide con base en su nivel de explotación, su facilidad de

propagación en el ecosistema, el daño realizado, el grado de control obtenido por el atacante, entre otros aspectos. El CVE igualmente agrupa las vulnerabilidades en "tipos" que nos permite asociar las vulnerabilidades a técnicas de ataques usadas por los ciberdelincuentes. Como se puede apreciar en la ilustración 7 tomada del sitio oficial del CVE – Mitre. [24]

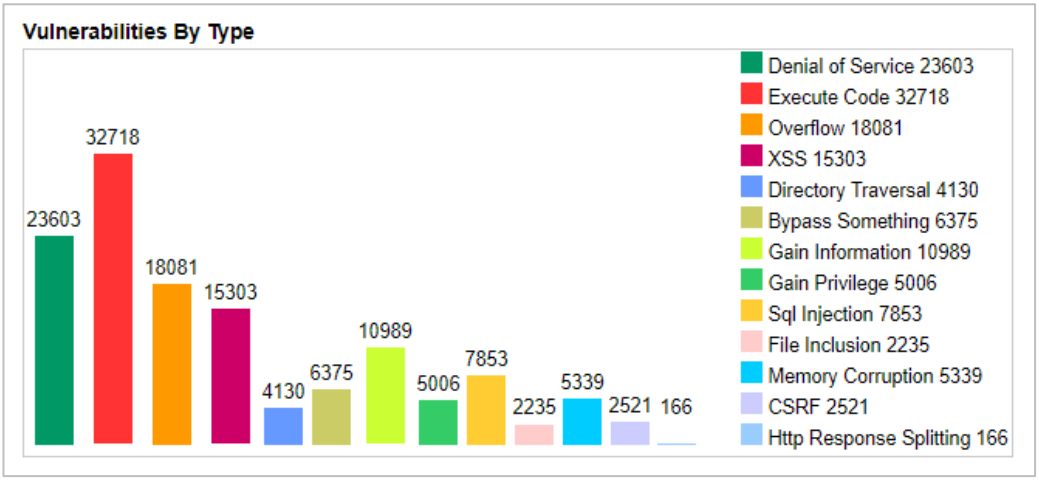

Ilustración 7 – Vulnerabilidades agrupadas por tipo. Mitre- CVE [24]

Cómo se puede apreciar, cada uno de los "Tipos" utilizados por MITRE se pueden asociar como un tipo de ataque que aprovecha vulnerabilidades técnicas para poder violentar el objetivo.

Igualmente relevante para el presente trabajo, fueron las técnicas de ataques descritas en el informe "The credential theft ecosystem" de la empresa Blueliv [20] y que cada una de ellas está especializada al robo de credenciales y no podemos dejar de mencionar la investigación profunda que realiza la empresa Verizon que en el año 2019 liberó al mercado un informe especial sobre las grandes brechas de seguridad y los diferentes tipos de ataques que se identificaron en ellas, denominado "2019 Data Breach Investigations Report" [18].

1.3 Identidad digital y modelos de IdM

Como se ha visto, en los últimos años se ha presentado un incremento significativo y constante de los servicios electrónicos sobre Internet, con énfasis en el aumento de transacciones financieras utilizando e-banking. A la par de dicho crecimiento, se observa igualmente, un aumento del cibercrimen, particularmente el robo de credenciales – cuyo destino final en muchas ocasiones, es la suplantación de la identidad digital en los sistemas para cometer todo tipo de ciberdelitos. En este punto, es relevante entonces profundizar en dos conceptos que son clave: La identidad digital y los sistemas de IdM (Identity Management)

1.3.1 El concepto de identidad digital

Para profundizar en el concepto de "identidad digital", vamos a retomar la conceptualización que se plantea en el trabajo "*Identity management systems: Laws of identity for models evaluation*" publicado en la IEEE por Hasnae L'Amrani y un grupo de investigadores de la universidad Mohamed de Marruecos, en el que nos brindan la siguiente definición:

> "*The digital identity is the representation of an active entity (Person, actor), it's used by most systems to allow access to resources. When users are involved in many domains they should hardly remember a lot of authentication criterions for every access. They exist many identity management systems that aim to solve the issues in relation with digital identity*." [25]. Que en español lo podemos traducir como: La identidad digital es la representación de una entidad activa (Persona, actor), ésta es usada por la mayoría de los sistemas para permitir el acceso a los recursos. Cuando los usuarios están involucrados en muchos dominios, difícilmente deberían recordar muchos criterios de autenticación para cada acceso. Existen muchos sistemas de gestión de identidad que tienen como objetivo resolver los problemas relacionados con la identidad digital.

Igualmente, encontramos elementos clave del concepto de "identidad digital" en la propuesta por Kim Cameron en su paper "The Laws of Identity":

> *"… digital identity as a set of claims made by one digital subject about itself or another digital subject*" [26]. Que en español lo podemos traducir como: ... identidad digital como un conjunto de afirmaciones hechas por un sujeto digital sobre sí mismo o sobre otro sujeto digital.

Partiendo de estas dos conceptualizaciones, podemos entonces decir que una identidad digital es la representación de una persona (o sistema) en el mundo digital y que puede ser identificada en forma única, dado un conjunto específico de características digitales que se pueden determinar en cada acceso o interacción con un sistema.

1.3.2 Factores de autenticación

Para crear una identidad digital, se requiere dotar a dicha identidad de un grupo de características o propiedades que le son exclusivas y que en combinación permiten identificarla, es así como se habla de factores de autenticación. Los factores de autenticación ideal se caracterizan por algo que sé sabe (contraseña), algo que se tiene (Token físico) y algo que se es (biometría) y esta triada se conoce como autenticación multifactor [27], tal y como se puede apreciar en la ilustración 8.

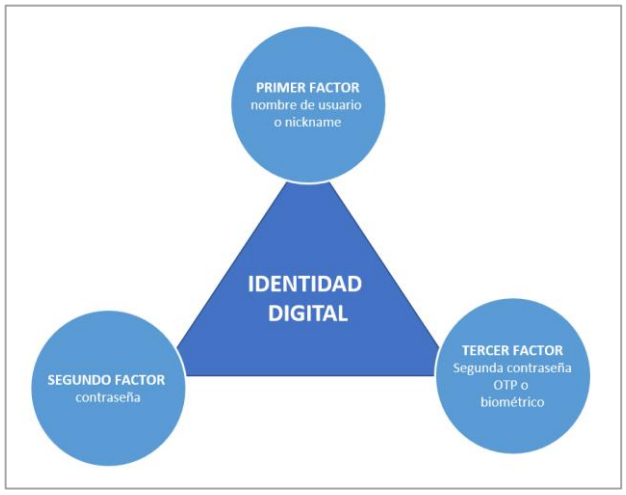

Ilustración 8 – Autenticación basada en 3 factores.

1.3.3 Las siete leyes de la identidad

Kim Cameron en el documento "*The Laws of Identity*" sostiene que durante la creación de Internet no fue definida una capa de autenticación nativa, es decir que los diferentes protocolos con los que nació Internet no regularon ni establecieron cómo resolver la pregunta: ¿Quién se está conectando a un recurso? - se focalizaron en el éxito de la transmisión de datos y la regulación y optimización de la conexión a través de las diferentes capas. Debido a esta ausencia, las diferentes soluciones de autenticación sobre internet que se han dado a lo largo del tiempo Cameron las considera como "parches" y obedecen más a diferentes desarrollos y modelos propietarios de diferentes actores que a una solución estandarizada y universal para todas las partes que utilizan Internet [26].

Es así como Cameron propone 7 leyes universales que debe cumplir un sistema de IdM y a continuación veremos un resumen cada una de estas leyes en la tabla 6.

LEYES DE LA IDENTIDAD	CARACTERÍSTICAS DE LA LEY
1. Control y consentimiento del usuario	El sistema debe revelar información, solo con el consentimiento del usuario.
	El sistema debe ofrece al usuario control de su información en todo momento.
	El usuario sabe si terceras partes están requiriendo/usando la información de su identidad.
2. Mínimo requerimiento y uso de la información y la autenticación del usuario	El sistema debe revelar el mínimo de información posible.
	El sistema debe revelar la información solo para casos de uso aprobados.
	El sistema debe almacenar la información mínima posible.
	El sistema debe minimizar los daños para el usuario ante posibles hackeos al propio sistema.
3. Justificación de uso	El sistema debe obrar solo cuando hay una justificación que así lo requiera.

	El consentimiento de uso por parte del usuario dueño debe ser ANTES de compartir o usar dicha información.
	El sistema debe facilitar la investigación ante las autoridades competentes.
4. Omnidireccionalidad	La autenticación debe ser en dos vías, de forma que el usuario tenga certeza de que se está autenticando en el sistema real.
	El sistema debe generar confianza para el usuario, previniendo posibles engaños de terceras partes. El usuario no debe tener dudas de que está en el sistema correcto.
5. Pluralismo de operadores y tecnología	El sistema debe ser compatible e integrable con otros sistemas de identidad, así mismo ofrecer protocolos y tecnologías abiertas para la conexión hacia él mismo.
6. Integración humana	El sistema debe ser compatible, amigable e intuitivo para los humanos
7. Consistencia en la experiencia de uso	El sistema debe ser coherente en la experiencia y forma de uso en cualquier contexto.

Tabla 6 – Resumen de las Leyes de la Identidad de Kim Cameron [26].

1.3.4 Modelos de IdM

Realizar un modelamiento de los esquemas de IdM que utilizan las diferentes soluciones comerciales permite comprender y agrupar dichas soluciones de acuerdo con su funcionamiento, sin la necesidad de analizar cada una de ellas – labor por lo demás imposible, toda vez que cada día surgen nuevas propuestas de IdM a nivel comercial. Crear este modelamiento facilita la realización posterior de comparaciones entre los diferentes modelos.

Se retoma una definición de "modelos de IdM" basada en la interacción de los actores (el usuario, la solución de negocio y el sistema manejador de identidades como tal) y el flujo de información. En este punto, se destaca el trabajo de investigación realizado por un grupo de profesionales de la universidad de Mohamed en Marruecos y publicado en la IEEE con el nombre "*Identity Management Systems: Laws of Identity for Models´s Evaluation"*, en este trabajo se formulan 4 modelos de IdM, se tipifica el funcionamiento y características de cada uno de ellos y finalmente se realiza una evaluación del cumplimiento de cada uno de los modelos contra las leyes de la identidad formuladas previamente por Kim Cameron. A continuación presentamos en la ilustración 9, los 4 modelos de IdM propuestos en esta investigación [28].

Ilustración 9 – Los 4 modelos de IdM propuestos desde la Universidad Mohamed [28].

1.3.5 Modelo de IdM aislado

Puede considerarse el modelo más usado y el origen de las diferentes soluciones de IdM. En este modelo, cada solución de negocio (sistema al que debe ingresar o interactuar el usuario) tiene una conexión directa con un único sistema administrador de identidades (IdM) y que solo atiende a esta solución de negocio en particular – es decir que la base de datos dónde se almacenan las identidades, la información asociada a dicha identidad y eventualmente los privilegios de acceso - solo le sirven a esta solución de negocio en particular.

La identidad es creada en el sistema de IdM propietario (paso 1) y es entonces almacenada en dicho sistema (paso 2); luego se le asignan al usuario credenciales para ingresar a la solución de negocio. Cada vez que el usuario ingresa a la solución de negocio debe suministrar las credenciales (paso 3) que a son recibidas y autenticadas por el IdM propio de la solución de negocio (paso 4) y finalmente se le concede acceso al usuario (paso 5) [28]. El modelo de IdM aislado lo podemos apreciar en la ilustración 10.

Observe como en el proceso, se repiten los mismos pasos para la solución de negocio 1 y para la solución de negocios 2.

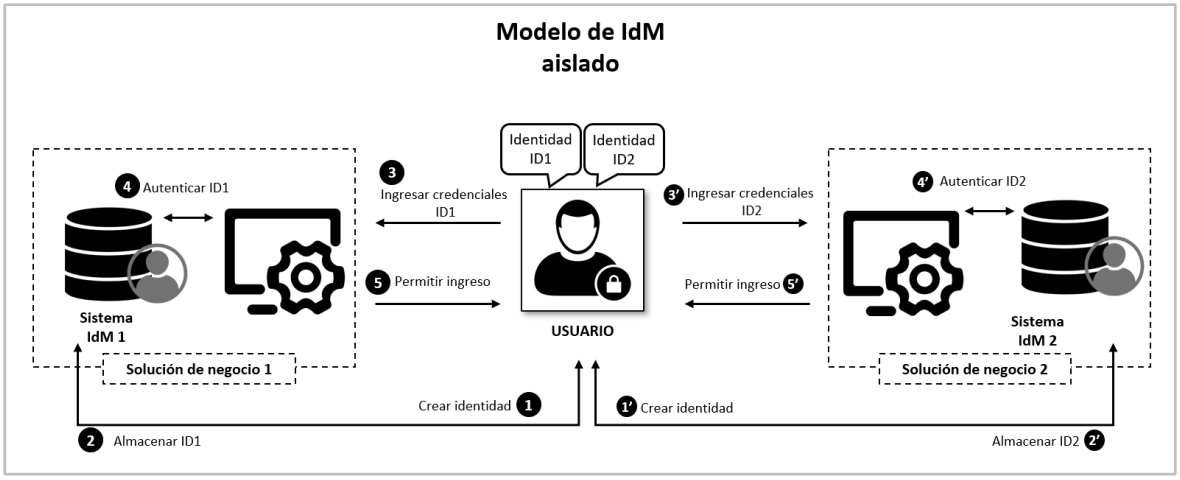

Ilustración 10 – Modelo de IdM aislado [28].

1.3.6 Modelo de IdM centralizado

En el modelo de IdM centralizado un mismo sistema administrador de las identidades (IdM) está conectado y ofrece sus servicios de autenticación a varias soluciones de negocio, de forma que el usuario puede ingresar a múltiples soluciones con la misma identidad (utilizando las mismas credenciales) las cuales le serán solicitadas en cada ingreso.

La identidad es creada en un sistema IdM (paso 1) y almacenada en el mismo sistema (paso 2), Así, cuando el usuario desea ingresar a la solución de negocio 1, ingresa las credenciales respectivas de

su identidad (paso 3), la solución de negocio las recibe y las pasa al sistema IdM para su autenticación (paso 4) y al recibir el mensaje de autenticación exitosa por parte del sistema IdM, otorga el acceso a la identidad (Paso 5). Cuando el usuario requiere ingresar a la solución de negocio 2, utiliza la misma identidad y el mismo juego de credenciales (paso 6), éstas son enviadas al sistema IdM para su autenticación (paso 7) y finalmente al comprobarse las credenciales, la solución de negocio 2 otorga acceso al usuario [28].

Una de las ventajas de este modelo es que la creación de identidad y asignación de credenciales solo se realiza una única vez y el usuario solo debe recordar un solo juego de credenciales – haciéndole la vida más fácil - sin embargo, esta misma lógica crea un punto de riesgo alto ante un robo de credenciales, pues las mismas credenciales otorgan acceso a múltiples soluciones de negocio. En la ilustración 11, podemos ver el funcionamiento del modelo de IdM centralizado.

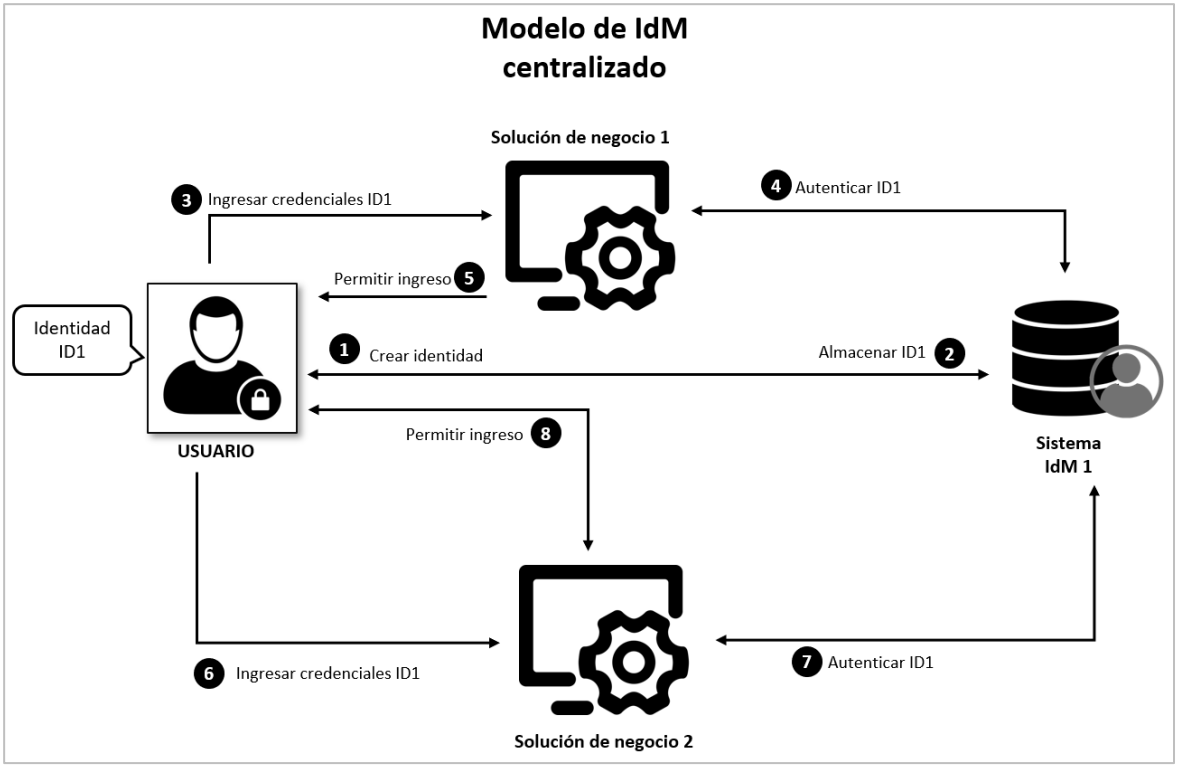

Ilustración 11 – Modelo de IDM centralizado [28].

1.3.7 Modelo de IdM centrado en el usuario

En este modelo, el usuario crea una identidad digital en un sistema de administración de identidades (paso 1); el sistema IdM crea la identidad pero no la almacena, sino que se la entrega al mismo usuario para que sea él quien la almacene y administre en su gestor local de administración de identidades (paso 2). Cuando el usuario desea ingresar a una solución de negocio, ésta le informa en que sistemas de administración de identidades confia y el usuario

selecciona en su programa de administración de credenciales local, la identidad que utilizará para autenticarse (paso 3). Así el gestor local de administración de identidades envía las credenciales de la identidad a la solución de negocio (paso 4). Finalmente, luego de validar que la identidad fue efectivamente autenticada contra el sistema IdM en el cual tiene una relación de confianza, otorga el acceso al usuario (paso 5). Nota: se repiten los mismos cinco pasos en cada solución de negocio que el usuario deba ingresar.

El modelo centrado en el usuario permite que el programa denominado *Gestor Local de IdM* pueda almacenar las identidades – casi como si fueran una especie de certificados digital (algo similar a la firma digital que se puede obtener en Colombia a través de Certicámara o una llave de autenticación almacenada en una Smart Card). De esta forma el usuario, quien finalmente es el propietario de la identidad digital, tiene control total sobre la identidad, quien la utiliza y cuando la está utilizando y le permite de igual forma custodiar los datos que conforman la identidad (como por ejemplo el correo electrónico, teléfonos, dirección, etc.) [28]. En la ilustración 12, se puede apreciar el modelo de IdM centrado en el usuario.

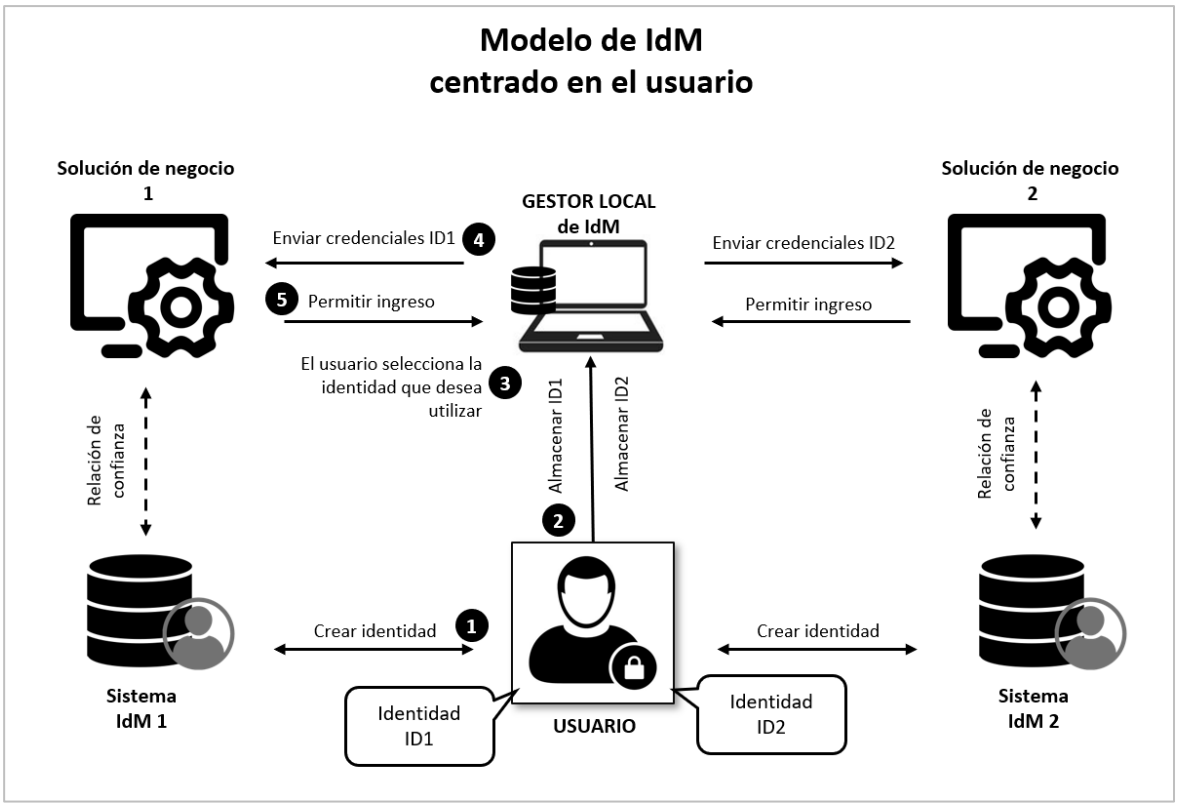

Ilustración 12 – Modelo de IdM centrado en el usuario [28].

1.3.8 Modelo de IdM federado

En este modelo, existe un sistema IdM contra el cual las diferentes soluciones de negocio establecen un dominio de confianza – esto quiere decir que van a confiar en la autenticación que realice dicho sistema y a permitir ingreso y accesos del usuario confiando en el "token" que entrega

el sistema IdM cuando se autentica; el token tiene un tiempo de vida limitado. Una característica importante de los sistemas federados es que trabajan bajo protocolos estandarizados (por ejemplo SAML, OAuth, OpenID, etc.) generando mayor transparencia e interconectividad entre los diferentes actores y permitiendo un servicio de autenticación agnóstico para múltiples soluciones de negocio.

El usuario crea la identidad en el sistema IdM (paso 1) y la identidad y sus datos son almacenados en dicho sistema (paso 2). Una vez creada la identidad, cada vez que el usuario se autentica en el sistema IdM (paso 3), éste le entrega de un token que es almacenado localmente por el usuario en el dispositivo que está usando (paso 4). Cuando el usuario ingresa a una solución de negocio que está en el dominio de confianza, le envía el token almacenado (paso 5) y de esta forma la solución de negocio verifica contra el sistema IdM la validez de dicho token (Paso 6) – si el token es validado por el sistema IdM, entonces se permite el ingreso e interacción del usuario con la identidad ya comprobada [28]. Este modelo de IdM federado se ilustra en la ilustración 13.

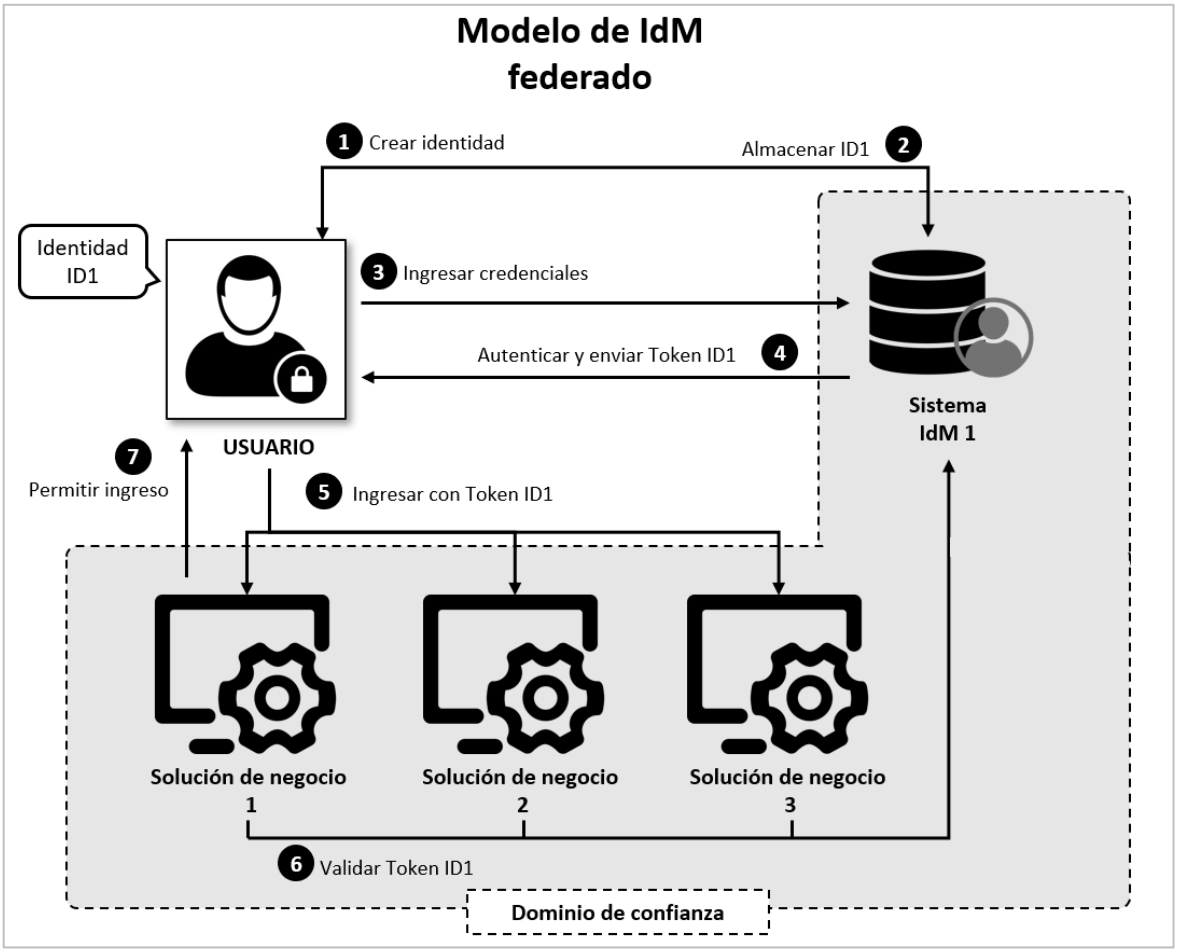

Ilustración 13 – Modelo de IdM FEDERADO [28].

1.3.9 Evaluación de los 4 modelos de IdM

La investigación realizada en *Identity Management Systems: Laws of Identity for Models´s Evaluation* nos presenta finalmente una comparación valiosa del nivel de cumplimiento de cada modelo sobre las siete leyes de la identidad, teniendo en consideración las características y forma de trabajo de cada uno de los estos modelos; de esta forma los autores concluyen que el modelo de IdM federado logra el mayor nivel de cumplimiento de las leyes de la identidad (4 de 7) y se presenta como el modelo más adecuado para las diferentes necesidades de manejo de identidades, resaltando sin embargo, que el modelo federado no permite control total de la identidad y de su información al usuario dueño de la misma y que en algunos puntos de la evaluación, los autores no contaron con suficiente información para calificar el cumplimiento o incumplimiento de ciertas leyes.

En la tabla 7, se presenta el resumen de esta evaluación y se utiliza la palabra "SI" para indica que el modelo si cumple la ley que se está evaluando; la palabra "no" se utiliza para indicar que el modelo no cumple con la ley que se está evaluando y la sigla "S/D" (sin datos) para indicar que los autores no tuvieron la información completa para evaluar el cumplimiento de la ley.

EVALUCIÓN DE LOS MODELOS DE IdM SOBRE LAS LEYES DE LA IDENTIDAD				
LEYES DE LA IDENTIDAD	**MODELO AISLADO**	**MODELO CENTRALIZADO**	**MODELO CENTRADO EN EL USUARIO**	**MODELO FEDERADO**
1. Control y consentimiento del usuario	NO	NO	SI	NO
2. Mínimo requerimiento y uso de la información	SI	S/D	S/D	SI
3. Justificación de uso	S/D	S/D	S/D	SI
4. Omnidireccionalidad	NO	SI	S/D	SI
5. Pluralismo de operadores y tecnología	SI	NO	SI	SI
6. Integración humana	SI	S/D	SI	S/D
7. Consistencia en la experiencia de uso	S/D	S/D	S/D	S/D

Tabla 7 – Comparación entre modelos vs. las leyes de la Identidad [28].

1.4 Principales soluciones de IdM tradicionales (no blockchain)

Una vez encontrada la forma de tipificar los modelos de IdM, se profundizó en algunas de las principales soluciones de IdM tradicionales que ofrece el mercado, detallando sus características y protocolos. En el mercado existen cientos de soluciones de IdM y para focalizar el esfuerzo, buscamos a un experto en clasificación, referenciación y comparación de soluciones tecnológicas a nivel mundial: Gartner. De acuerdo con el cuadrante mágico de Gartner del año 2019 para soluciones de "*Access Management"*, están son las 5 soluciones de IdM más representativas el mercado, como nos muestra la ilustración 14 en el cuadrante de líderes.

Ilustración 14 – Cuadrante mágico de Gartner [29].

Se pueden observar 14 soluciones de IdM que Gartner define como las más representativas de la industria. A continuación, vamos a profundizar un poco más en las 5 principales, considearadas por este organismo de consultoria, como las soluciones líderes en el mercado.

1.4.1 Okta Authentication

Okta es uno de los principales proveedores independientes de identidad. Sus soluciones ofrecen más de 6.500 integraciones preconstruidas para aplicaciones y proveedores de infraestructura y en la actualidad la compañía tiene soluciones de IdM en casi 8,000 organizaciones alrededor del mundo, incluidas JetBlue, Nordstrom, T-Mobile, Twilio, entre muchas otras [30]. Sus soluciones se orientan tanto a la protección de identidades de empleados como a la protección de identidades para clientes.

Okta Authentication es el producto de IdM de la compañía Okta para la autenticación de clientes, ofrece una versión para trabajar en nube llamada Okta Identity Cloud o la solución clásica para operar desde las instalaciones del cliente (On premis), es compatible con estándares de autenticación SAML, OAuth 2.0, OpenID, OIDC, entre otros; facilitando la integración con otros sistemas IdM abiertos como Facebook, Google, Microsoft, Twitter, etc. La solución cuenta con más de 6.000 conectores para todo tipo de aplicaciones y soluciones comerciales y permite funciones avanzadas de single sign on (SSO), autenticación basada en riesgo, OTP, reportería e integración con sistemas tipo SIEM. En general es una de las soluciones de IdM más versátiles y completas del mercado [31]. La arquitectura de Okta se aprecia en la ilustración 15, a continuación.

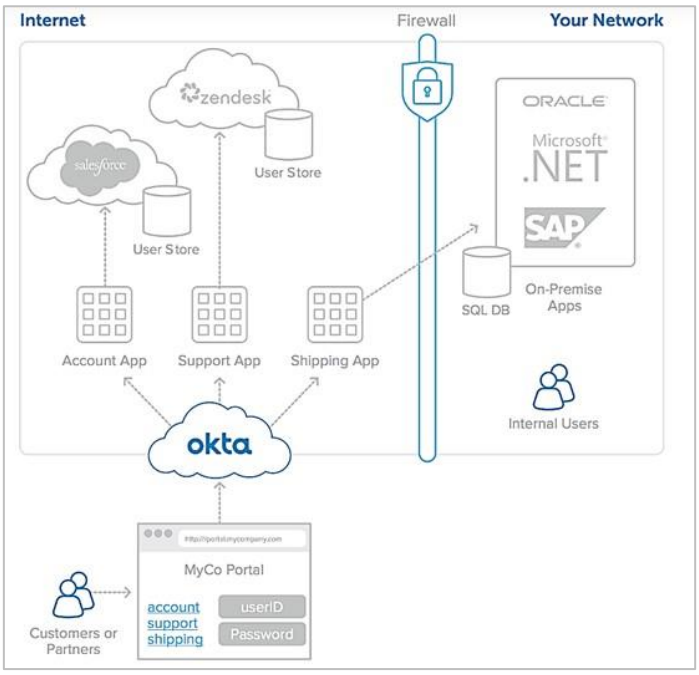

Ilustración 15 – Arquitectura de *Oka Authentication* para portales de clientes. Oka [31]

1.4.2 Microsoft Identity Manager

Microsoft Identity Manager (MIM) 2016 es la solución especializada en IdM del gigante Microsoft, está orientada al manejo de usuarios, políticas y accesos dentro de las organizaciones, aunque igualmente sus capacidades se pueden adaptar para la integración con portales y servicios de cara a Internet, incluyendo la capacidad de ser utilizado para soluciones de negocio con autenticación de clientes o en soluciones hibridas. Ofrece la posibilidad de integrarse con otros sistemas de IdM y manejar One-Time Password (OTP), SSPR Short Message Service (SMS), integración nativa con Azure AD y las diferentes soluciones de Microsoft en la nube – por ejemplo Office365 y soporta estándares de conexión como LDAP v3, SOAP, DSML, LDIF, entre otros [32].

En esta arquitectura se cuenta con el servicio MIM (Microsoft Identity Manager) conectándose con la base de datos centralizadora de identidades – denominada MIM sync Service and database, la cual a su vez interactúa con los servicios de directorio activo propios de Microsoft y con el componente web denominado MIM Portal – el cual permite interacción con los clientes finales de la solución, que para el caso pueden ser las diferentes versiones de los sistemas operativos Windows o para otro tipo de sistemas como Linux, los diferentes clientes de conexión ofrecidos por Microsoft [32].

Veamos a continuación, en la ilustración 16, la arquitectura general del modelo de MIM de Microsoft y la forma en que se interconectan sus componentes.

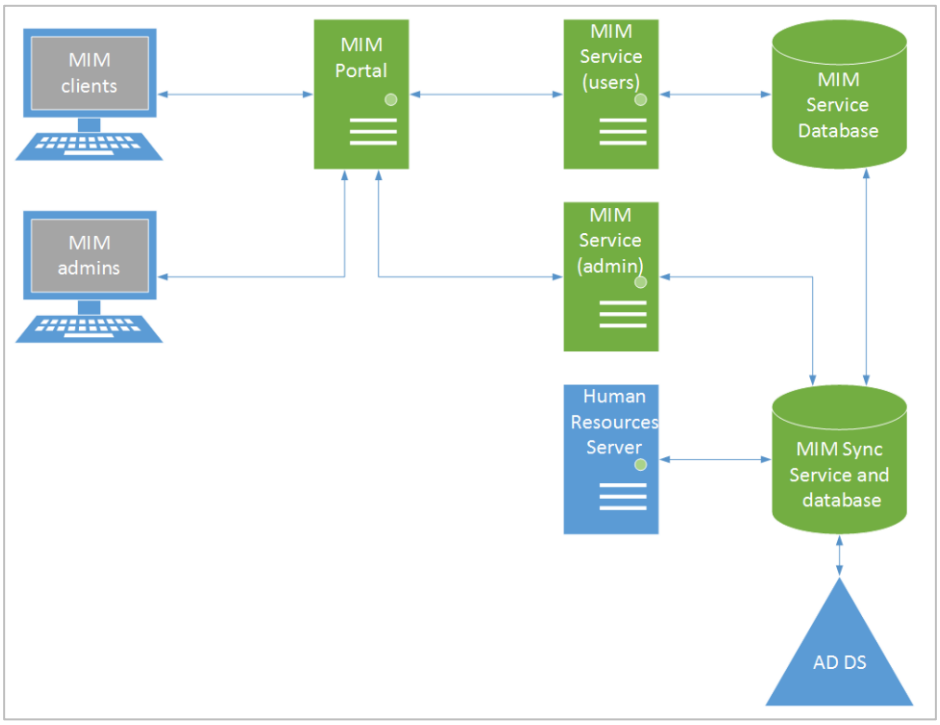

Ilustración 16 – Arquitectura de *Microsoft Identity Manager.* Microsoft [32]

1.4.3 Ping Identity Platform

Ping Identity es una compañía americana con presencia en la bolsa de valores de Nueva York, fue creada en el año 2002 en Denver, Colorado y en la actualidad tiene presencia en 6 países alrededor del mundo. Está completamente dedicada a desarrollar soluciones de control de acceso y ofrece 5 diferentes tipos de productos de IdM orientados a resolver necesidades empresariales y gubernamentales. [33].

Dado que la presente tesis está focalizada en IdM para portales de e-banking, vamos en consecuencia a centrarnos en la solución de Ping Identity llamada *Customer360* la cual está dirigida a la autenticación de clientes. Esta solución se ofrece como SaaS, On premis o en una arquitectura hibrida. Entre sus principales características tenemos: Integración con redes sociales (Facebook, Google, Microsoft, entre otros), autenticación sin password, recuperación de cuenta, MFA, integración nativa vía APIs con AWS, Azure, IBM, entre otros servicios de nube, compatibilidad con protocolos SAML, WS-Trust, SOAP, entre otros y administración centralizada de políticas así como un módulo analítico de seguridad y comportamiento de los clientes [34]. Podemos clasificar esta solución como un modelo IdM Federado o Aislado - de acuerdo a la forma de implementación y a las características flexibles que ofrece la solución. Su arquitectura se muestra en la ilustración 17.

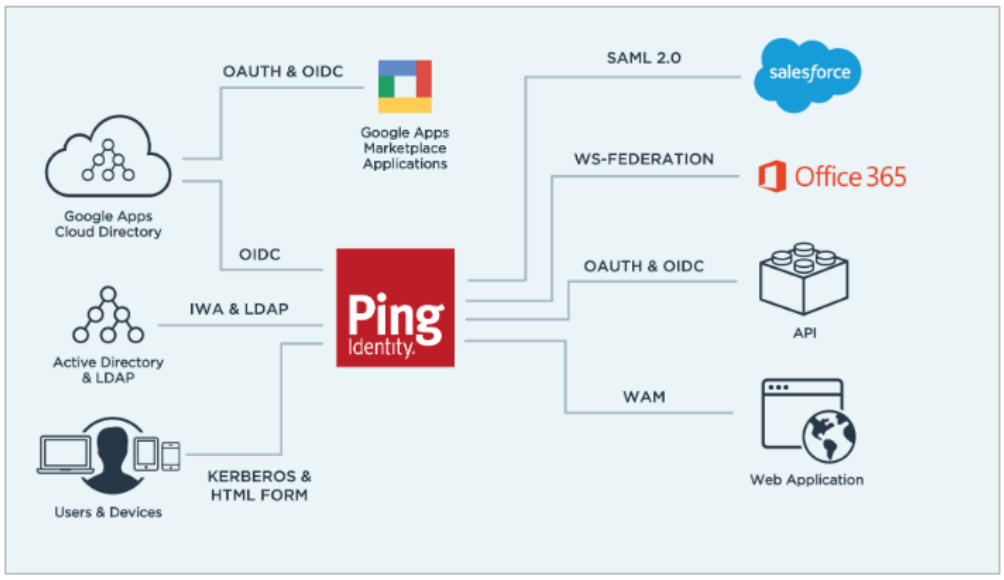

Ilustración 17 – Modelo de *Ping Identity Platform*. Ping Identity [34]

1.4.4 IBM Identity and Access Management

IBM es un fabricante de múltiples soluciones tecnológicas y en la actualidad ofrece en su portafolio comercial un conjunto de productos especializados para la gestión, administración y monitoreo del manejo de las identidades digitales. Considerando el enfoque en IdM para e-banking, se toma en particular el producto Adaptive authentication que provee servicios de manejo de identidades, enrolamiento, autenticación con o sin password, MFA, monitoreo y respuesta dinámica ante el riesgo durante la autenticación. Es compatible con los protocolos SAML, FIDO2, OAUTH 2.0, OIDC, entre otros y se ofrece al mercado en modalidad On Premis, híbrida o cloud (SaaS) usando un módulo denominado Cloud Identity for Consumers [35] . Veamos la arquitectura general de la solución en la ilustración 18.

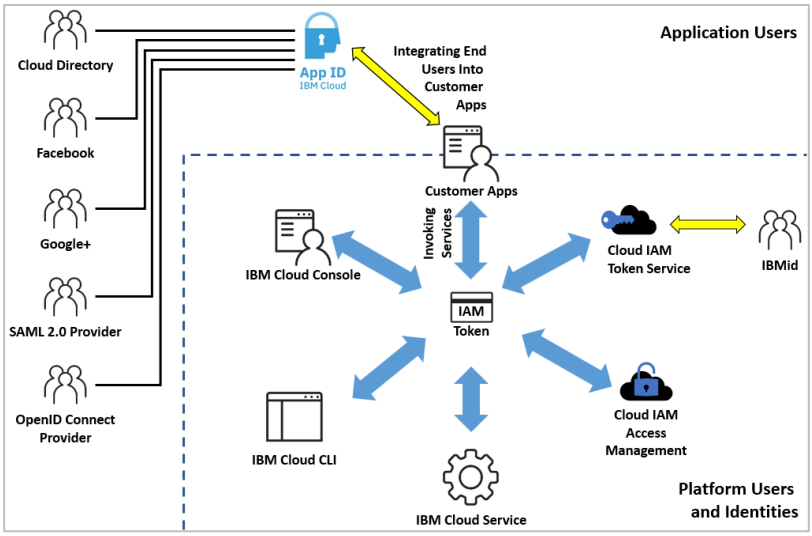

Ilustración 18 – Modelo de *IBM IAM*. Smolny [35]

1.4.5 Oracle Identity Management

Oracle Identity Management está orientado al entorno organizacional gestionando el ciclo de vida de extremo a extremo de las identidades de los usuarios, empleados y proveedores en todos los recursos de la empresa, tanto dentro del perímetro como en los diferentes servicios de nube que ésta maneje. La plataforma Oracle Identity Management ofrece módulos que cubren el gobierno de la identidad, la gestión de accesos y los servicios de directorio. Esta plataforma permite fortalecer la seguridad, simplificar el cumplimiento normativo y controlar los accesos a soluciones móviles y de redes sociales. Igualmente Oracle cuenta con un servicio de gestión de identidad y acceso a través de una plataforma en la nube denominado Oracle Identity Cloud Service. Entre las principales características de Oracle Identity Management tenemos manejo de la Gobernanza o gobierno de las identidades, portal unificado de accesos - integrado a los principales sistemas empresariales, bases de datos y portales de colaboración internos y externos [36], como se puede apreciar en la ilustración 19.

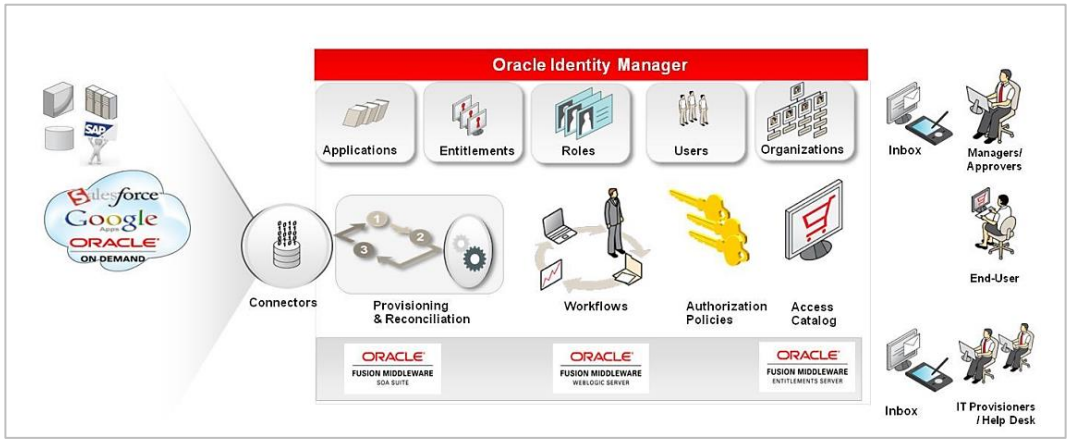

Ilustración 19 – Esquema de Oracle Identity Management. Oracle [36]

1.5 Principales soluciones de IdM sobre blockchain

La aparición de blockchain ha venido generando nuevos tipos de soluciones para diversos retos de la sociedad, es así como en el mundo de las soluciones de IdM también han venido surgiendo nuevas soluciones sobre blockchain. Antes de profundizar en algunas de ellas y considerando lo nuevo que pude ser blockchain, a continuación tendremos una breve descripción de qué es y cómo funciona blockchain.

1.5.1 Entendiendo blockchain

Para entender mejor el concepto de blockchain vamos a tomar el artículo "*Blockchain Technologies: The Foreseeable Impact on Society and Industry*", en el que se describe esta tecnología como un conjunto de transferencias electrónicas que utilizando certificados digitales permite firmar y garantizar la integridad de cada transacción. Cada transacción a su vez es registrada en un libro de

estado de cuentas o DLT - por sus siglas en inglés (Distributed Ledger Technology) - y de esta forma se logra fidelidad de cada entrada y salida de la información que se ha registrado. Adicionalmente se utiliza un sello de tiempo por medio de un "time stamp server para garantizar la integridad de las transacciones en el tiempo y eliminar el riesgo de una doble transacción (conocido como doble pago o double spend); todo esto funciona a través de un modelo con múltiples computadoras conectadas a internet operando en conjunto, como nodos distribuidos - tipo redes P2P - de un mismo sistema, lo permite una alta tolerancia a fallos.

Para cerrar el ciclo, esta misma estructura de nodos, se encarga de garantizar por conceso matemático la integridad y la confidencialidad de la información creando bloques electrónicos de transacciones que se firman digitalmente y se enlazan uno con otro (cadena de bloques) y se actualizan en todos los nodos de la red, de forma que mientras más grande es la red y más bloques tiene, es más segura por sí misma, sin la necesidad de un tercero de confianza [37], como se muestra en la ilustración 20.

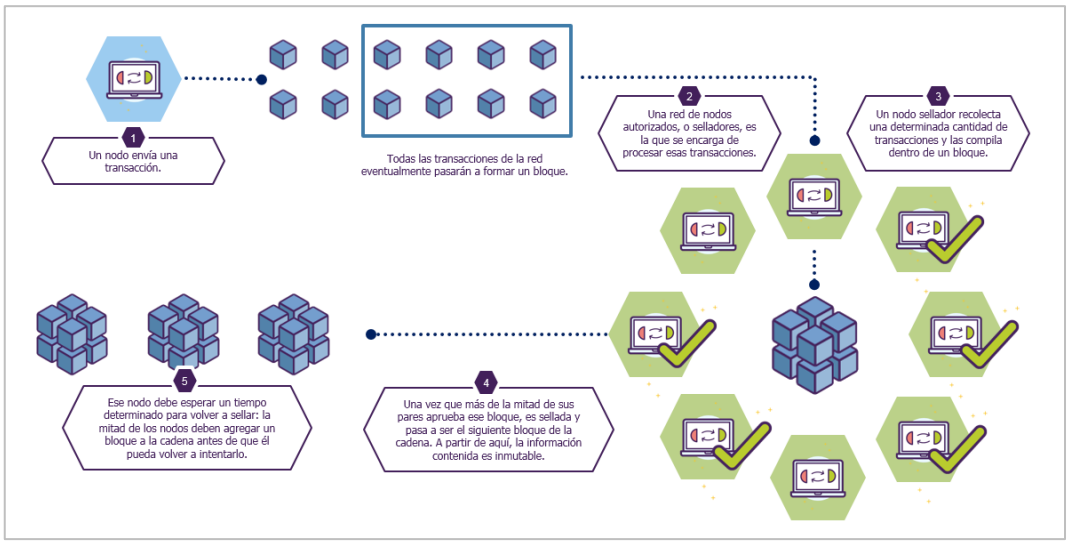

Ilustración 20 – Esquema conceptual del funcionamiento de blockchain. Fuente: BFA [38]

Una mirada holística de todo el potencial de blockchain la encontramos en el trabajo de investigación "*Blockchain Technologies: The Foreseeable Impact on Society and Industry"* que, desde el University College London, nos ofrece detalles sobre el funcionamiento de blockchain, los conceptos claves de su arquitectura y las diferentes perspectivas, retos y oportunidades que ofrece a la industria, a la academia, a los equipos de innovación y al sector gobierno frente a esta nueva arquitectura [37].

Esta tecnología está despertando tal interés en la sociedad, que el trabajo de Matteo Gianpietro "*50+ Examples of How Blockchain are Taking Over the World*" nos permite conocer con mayor detalle, las empresas, los gobiernos, las universidades y los equipos de investigación que están adelantando soluciones sobre blockchain. En su artículo Gianpietro compara el nacimiento de blockchain con el nacimiento de una segunda versión de internet y pronostica toda una revolución social e industrial en las próximas décadas a partir de esta tecnología y enumera y describe

alrededor de 50 soluciones de IdM que ya están en fase de desarrollo o en producción, incluyendo algunas de las más adelantadas a nivel de IdM [39].

Igualmente relevante resulta la investigación de los doctores Paul Dunphy y Fabien Petitcolas quienes nos presentan una mirada más profunda sobre la administración de identidades basada en blockchain; en su artículo "*A First Look at Identity Management Schemes on the Blockchain"* publicado en la IEEE, exploran con profundidad las características de tres de las principales soluciones del mercado: uPort, Sovrin y ShoCard - que de acuerdo con su investigación – pueden ser consideradas las 3 mejores exponentes de soluciones de IdM sobre la tecnología de bloques [40] y que profundizaremos más adelante en este mismo trabajo.

Al ser blockchain una nueva tecnología, es importante conocer no solo sus características sino también fortalezas y debilidades. De acuerdo con Brian Scriber en su artículo *A Framework for Determining Blockchain Applicability* debemos evaluar aspectos críticos a la hora de seleccionar blockchain como una arquitectura objetivo para una solución tecnológica. Algunos de los aspectos principales que se resaltan en la investigación son: Al utilizar blockchain se debe tener en cuenta el alto costo en capacidad de cómputo requerido debido a su comprobación matemática de los hashes de cada bloque. Otro aspecto a tener en consideración es la inalterabilidad del sistema – que dependiendo la necesidad, puede ser una ventaja o una desventaja, pues un sistema inalterable no puede por ejemplo corregir errores de digitación o hacer reversiones en una transacción. La velocidad transaccional es otra característica crítica, pues los cálculos de blockchain pueden ser demasiado pesados y lentos para soluciones que requieran procesamiento en tiempo real – como por ejemplo control sobre redes SCADA. Finalmente la capacidad de escalamiento que conlleva la red de nodos en un sistema blockchain implica también cierta pérdida de control sobre los nodos que se están admitiendo en la red [41].

En resumen, las soluciones basadas en blockchain ofrecen por sí mismas confidencialidad, integridad y disponibilidad, lo que las hace atractivas para desarrollar soluciones de identidad digital.

1.5.2 Relación entre blockchain y las soluciones de IdM

Una vez comenzamos a entender mejor el funcionamiento y la arquitectura de blockchain, vamos a profundizar ahora en algunas de sus características que se acoplan a la naturaleza misma de un sistema de IdM y que están muy bien descritas en el trabajo *A First Look at Identity Management Schemes on the Blockchain* [40].

Descentralizado, blockchain en su naturaleza misma está construido para compartir la información y aprobar las transacciones por diferentes nodos, lo que en esencia permite un sistema descentralizado en el cual las partes pueden constatar por sí mismas la consistencia de la información.

Integridad del tiempo; al utilizar un sistema de firma de tiempo (time stamp) para registrar los diferentes eventos o transacciones, se garantiza la sincronización de los relojes y la inalterabilidad de los registros asentados.

Inclusivo, podemos decir que blockchain permite proponer nuevas formas de manejar la identidad digital, incluyendo formas modernas de interacción con los diferentes sistemas.

Costo-efectivo, dada la naturaleza distribuida de blockchain, en la que el costo de computación y almacenamiento se puede distribuir en diferentes nodos o actores, podemos aprovechar esta capacidad para construir soluciones escalables a costos razonables.

Control del usuario, debido a la transparencia del código, la criptografía y los algoritmos utilizados en las soluciones basadas en blockchain, el usuario final puede tener mayor conocimiento y por lo tanto mayor control de su información y la manera que está siendo utilizada por parte del sistema.

Es así como podemos entonces encontrar características naturales de la arquitectura de blockchain que pueden facilitar la construcción de sistemas IdM de forma novedosa, segura y costo eficiente. Es por este motivo que en el siguiente apartado, vamos a profundizar en tres tecnologías que han venido destacándose como soluciones de IdM sobre blockchain.

1.5.3 Concepto de Identidad auto soberana

La aparición de blockchain permite materializar un concepto que ha venido desarrollándose en los últimos años: la identidad auto soberana o "self sovereign identity" como se denomina en inglés. La identidad auto soberana permite que el propietario de la identidad tenga control total sobre el uso que se le da a ella, es quien decide cuando crearla, sabe quién está utilizando su identidad o requiriendo autenticarla y además tiene el control de la información o atributos de la identidad que soluciones de negocio están utilizando, todo esto en un sistema tecnológico que es transparente y deja registro permanente de la forma y quienes utilizan dicha identidad. Adicionalmente el sistema que administra las identidades no es de propiedad de las soluciones de negocio que lo utilizan, se podría decir que es un sistema público o abierto que no tiene un "dueño corporativo".

Este modelo está más ampliamente descrito en el white paper "*The Inevitable Rise of Self-Sovereign Identity*" [42], igualmente encontramos detalles de su funcionamiento y filosofía en el white paper "*uPort_whitepaper_DRAFT20161020*" [43] y en "*Civic - Whitepaper*" [44].

1.5.4 Soluciones de IdM sobre blockchain

En la actualidad existen múltiples soluciones, iniciativas, proyectos o pruebas de concepto sobre soluciones de IdM en blockchain, la mayoría de ellas basadas en el concepto de identidad auto soberana, entre ellas podemos listar uPort, Sovrin, ShoCard, Civic, OneName, World Citizenship,

Blockstack, etc. Sin embargo para la presente investigación seleccionamos aquellas que más han avanzado en la construcción de un ecosistema abierto (su código fuente es de libre acceso) y que ofrecen recursos estandarizados para su utilización comercial o pública (librerías, Apis y SDK). Así pues, se va a profundizar en: uPort, Sovrin, ShoCard y Civic, como representantes de las soluciones de IdM sobre blockchain.

1.5.5 uPort

uPort es una compañía Norte Americana con sede en Brooklyn, New York, fundada en el 2016 con capital privado y que se especializa en la construcción de soluciones para el manejo de la identidad digital sobre blockchain. La compañía ofrece 2 productos específicos: uPort open y uPort Serto. El primero es en general el ecosistema de autenticación y el segundo es la App disponible para interactuar con el sistema de autenticación [45].

uPort Open

Es un modelo de solución de IdM descentralizado, construido sobre la plataforma de blockchain Ethereum, con una arquitectura que permite generar autenticación compatible con sistemas de e-banking y otras aplicaciones de cara a internet. En general uPort trabaja con tres componentes principales: Los "Smart contracts", las librerías para desarrolladores y la app para dispositivos móviles.

uPort es de código abierto y se encuentra disponible en el repositorio oficial de Github de uPort (https://github.com/uport-project), consiste en una series de librerías y rutinas de programación en las que las identidades están representadas por identificadores descentralizados (DID) que siempre son creados por los propios usuarios - esta es una norma propuesta del Grupo de Trabajo de Reclamaciones Verificables del W3C y se basa en el estándar *ERC1056 Lightweight Ethereum Identity*, que uPort propone como un estándar común de Ethereum para implementar Ethereum Wallets. Finalmente, el modelo de reclamos verificables se basa en los tokens web JSON (JWT) estándar de IETF. [46]

En la actualidad el manejo de identidad basado en el modelo de uPort está siendo utilizada en la *Global Legal Entity Identifier Foundation* (GLEIF) – organismo sin ánimo de lucro de carácter supranacional con sede en Basilea, Suiza y que representa a las autoridades públicas del mundo que han unido sus fuerzas para impulsar la creación de una base de datos abierta para la identificación de personas jurídicas en el seno de los mercados financieros globales [47]. uPort también fue integrado en el proyecto Onfido. Este proyecto propone un nuevo estándar de identidad para renovar toda la autenticación sobre Internet, fue desarrollado en unión con la consultora internacional PwC, la universidad de Oxford y el fondo de inversión de Microsoft. Onfido ofrece seguridad durante el proceso de enrolamiento de los clientes del sector bancario [48].

En la ilustración 21 a continuación, podemos apreciar una descripción general de la arquitectura de uPort y de los principales componentes del modelo de servicio que corren sobre blockchain en Ethereum y que en la gráfica son identificados como “Servicios Centrales” [43].

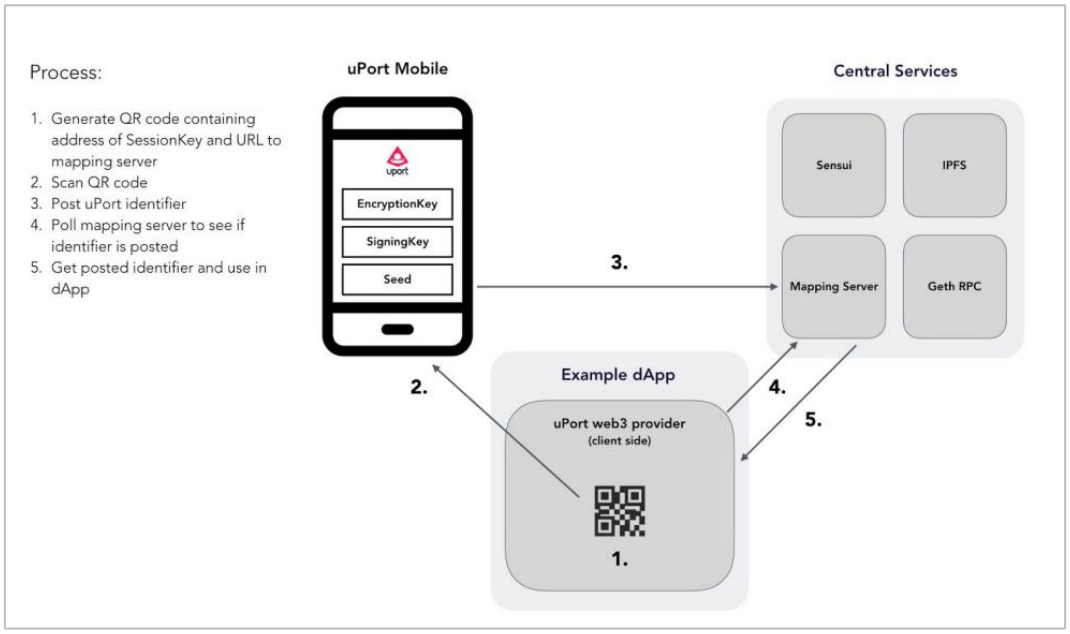

Ilustración 21 – Arquitectura de uPort. uPort_whitepaper_DRAFT20161020 [43].

1.5.6 Sovrin

Igual que uPort, la visión de Sovrin está construida sobre el concepto de Identidad Autónoma Soberana o self-sovereign identity – en inglés, en el que cada persona es dueña y responsable de la generación y utilización de su identidad digital, construida al mismo tiempo, sin un sistema u organismo centralizador. El primer componente de su arquitectura está definido por la Fundación Sovrin – que es un organismo global agnóstico de gobiernos u organizaciones y que tiene por objetivo la gobernanza de la red de identidad de Sovrin. Esta Gobernanza reconoce dos tipos de actores: Los Miembros (que básicamente es cualquier persona o dispositivo que posea una identidad dentro de la red de identidad de Sovrin y los “Stewards” o custodios – que son instituciones de confianza (como organismos gubernamentales, universidades, entidades financieras, etc. – que suministran la infraestructura distribuida de nodos de la red de Sovrin y se rigen bajo los parámetros de la Fundación Sovrin.

Adicionalmente Sovrin está conceptualizado como un sistema de Libro Mayor autorizado por el público. La arquitectura general de Sovrin se compone de tres capas: Sovrin Ledger, Sovrin Agents y Sovrin Clients. Estas capas se pueden apreciar en la ilustración 22.

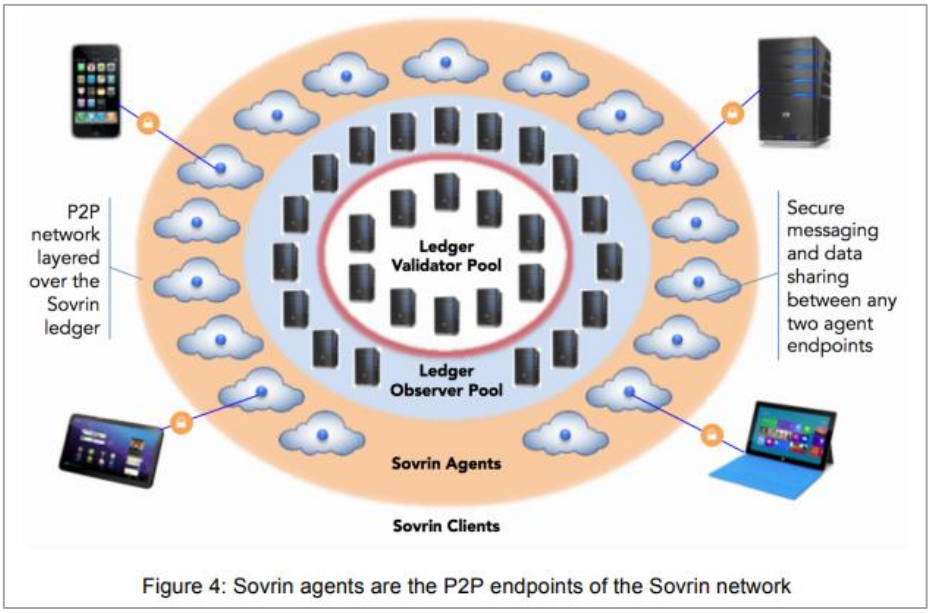

Ilustración 22 – Arquitectura de Sovrin. Sovrin [49]

A continuación vamos a realizar una descripción de cada una de las capas y de sus funciones principales.

Sovrin Ledger: Es el componente base de toda la solución, en esta capa se maneja el libro root de registro de identidades, es decir dónde se registran las identidades de cada propietario (persona o dispositivo) y es mantenido en su estructura por diferentes instituciones a nivel mundial llamadas "Stewards" o custodios". De igual forma, desde esta capa se maneja la gobernanza y estructura de código abierto de Sovrin a través de la *Fundación Sovrin*.

Sovrin Agents: Esta capa permite que las personas y a las diferentes empresas personalizar las reglas de negocio en la forma de tratar la identidad y la autenticación, incluyendo la capacidad para intercambiar procesos de autenticación, manejar las llaves diferentes llaves del propietario de la identidad y registrar y mostrar la trazabilidad de cada uso de la identidad en el ecosistema de Sovrin y sus miembros.

Sovrin Clients: Esta capa corresponde a la porción de código (aplicación en dispositivos móviles o también de computadores) que se encarga de crear la interfaz con el usuario, normalmente como una App en un dispositivo móvil. La ilustración 23 representa la forma cómo funciona un ecosistema de autenticación basado en Sovrin.

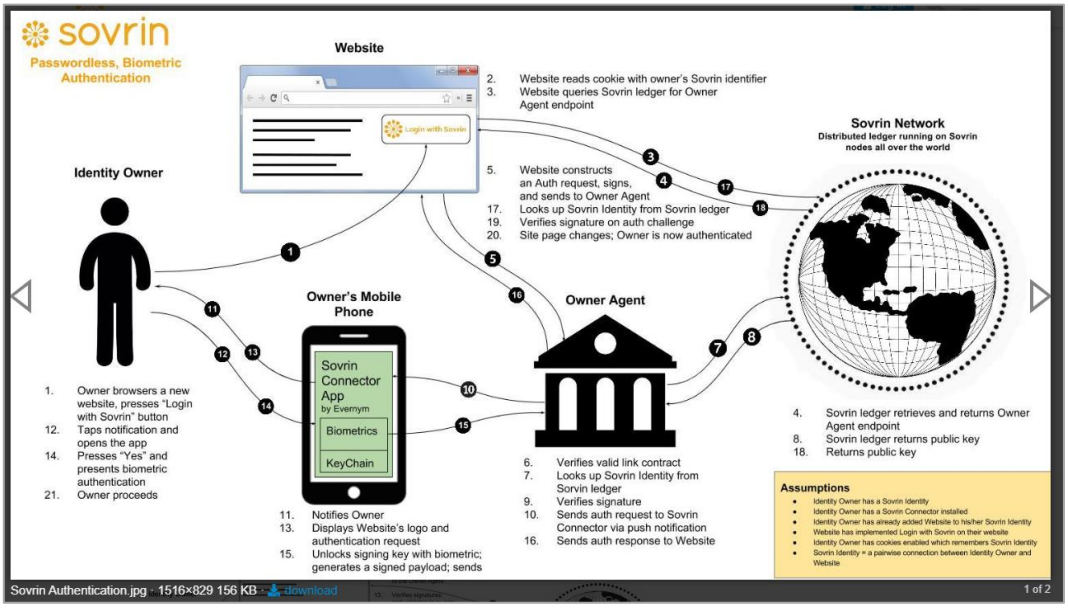

Ilustración 23 – Autenticación usando Sovrin. Sovrin [50]

1.5.7 ShoCard

ShoCard es una solución de IdM que puede ser implementada sobre diferentes plataformas de desarrollo en blockchain, por ejemplo Ethereum, BlockCypher, Amazon Managed Blockchain, entre otras. La empresa (ShoCard Inc.) fue fundada en el año 2015 con sede en Cupertino – California y su fundador y CEO Armin Ebrahimi basó el enfoque de ShoCard en el concepto de una plataforma de autenticación digital que funciona similar a la forma como se utiliza hoy en día una licencia de conducción como prueba de identificación personal en el mundo físico – sobre todo en el marco de los Estados Unidos. ShoCard pues permite digitalizar un documento de identidad personal (como la licencia de conducir, el carnet de seguridad social, el pasaporte, etc.) y asociarle elementos adicionales de identificación – como registros biométricos para poder crear una tarjeta de identidad digital basada en criptografía sobre blockchain. Dicha identificación digital permite ser usada como una prueba de la identidad de la persona ante una transacción digital usando el documento digitalizado y firmado a través de criptografía y biometría y al mismo tiempo facilitarle al dueño de la identificación el control total de la información que está compartiendo, todo esto a través de través de una app que almacena la tarjeta digital de identidad, gestiona las solicitudes de autenticación al momento de ser requerida - sin necesidad de enviar el documento de identidad digitalizado originalmente (escaneado) - sino solo una autorización "cifrada" desde la identidad base.

Para profundizar en el funcionamiento de ShoCard podemos partir de la descripción que nos presenta Koshik Raj en su estudio Foundations of blockchain [51] sobre funcionamiento de esta solución y su estructura de 5 capas lógicas, que se puede apreciar en la ilustración 24.

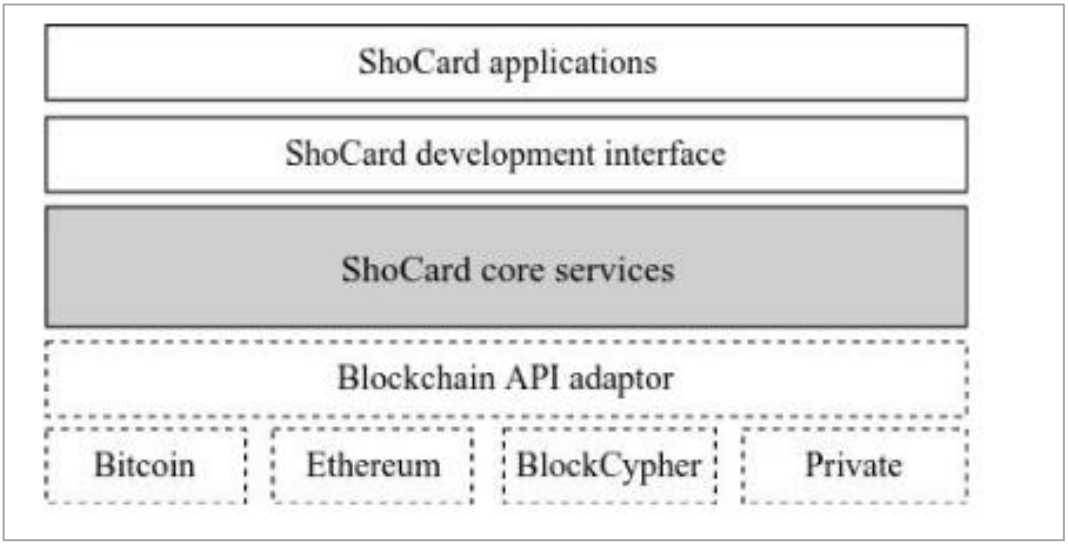

Ilustración 24 – Capas lógicas de ShoCard. Raj [51]

De acuerdo con la gráfica anterior, tenemos la capa de usuario final: *ShoCard applications*, es la App que corre sobre el dispositivo móvil y que le permite al dueño de la identidad escanear un documento de identificación personal, cifrarlo y firmarlo digitalmente con su juego de llaves público/privado para luego ser utilizado como mecanismo de autenticación en los diferentes sistemas conectados al core de ShoCard.

Luego tendemos la capa dónde se desarrollan las interfaces de conexión e intercambios del sistema: *ShoCard development interface*. La capa de *ShoCard core services* permite manejar las reglas de custodia y verificación criptográfica de la autenticación sobre la red blockchain. Esta capa a su vez se soporta sobre un conjunto de APIs que regulan el funcionamiento de la red de blockchain sobre la que se está corriendo (por ejemplo Ethereum, BlockCypher, etc) y que se denomina *Blockchain API adaptor*, permitiendo de esta forma que ShoCard pueda funcionar en diferentes tipos de redes blockchain. Finalmente tenemos la capa de infraestructura y protocolos propios del dueño de la red de blockchain, a la que podríamos denominar como el *network blockchain provider.*

En la ilustración 25, veremos la arquitectura general de la solución ShoCard presentada en el artículo científico *DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network* por Jamila Alsayed Kassem y otros investigadores [52].

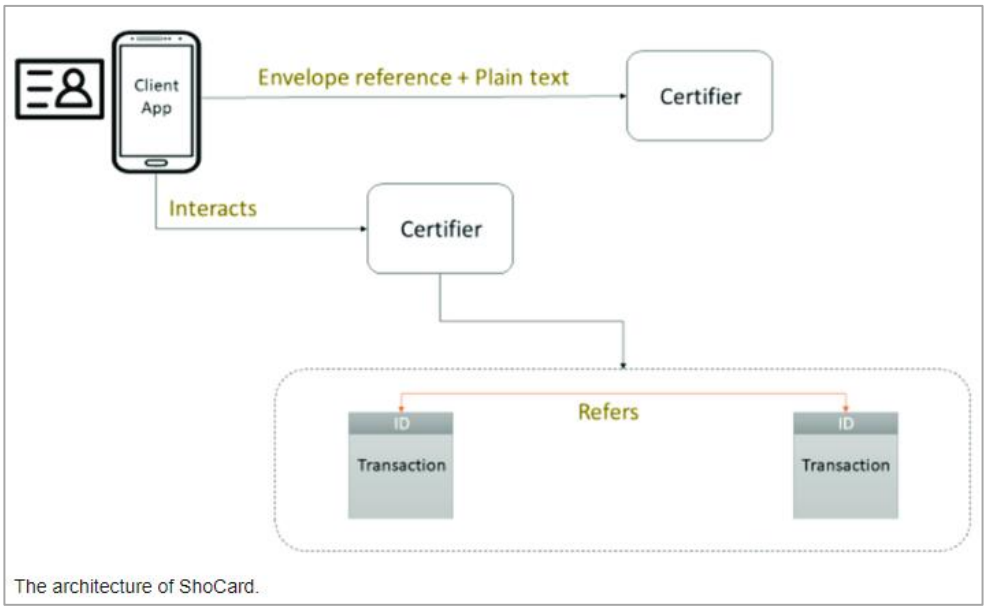

Ilustración 25 – Arquitectura tecnológica de ShoCard. Alsayed [52].

Recientemente, en marzo de 2020, la empresa *ShoCard Inc* fue adquirida por la empresa *Ping Identity* – que recordemos, se encuentra entre las principales proveedoras de soluciones de identidad tradicionales (ver capítulo 1.4.3 en este mismo documento) y esto ha generado el cierre de documentación, librerías y recursos de desarrollo (SDK) públicos, de forma que está por definirse el futuro comercial de la solución de ShoCard. [53]

1.5.8 Civic

Uno de los jugadores más recientes en el mundo de IdM sobre blockchain es la empresa *Identity Technologies, Inc.*, una organización sin ánimo de lucro fundada en el año 2018 con sede en San Francisco – California y enfocada en la generación de sistemas de identidad de uso libre; ofrece una serie de recursos y librerías para desarrollar un ecosistema de identidad sobre las redes de blockchain Ethereum y Bitcoin [54]. Actualmente está disponible en App Store y Google Play Store una aplicación para dispositivos móviles desarrollada por esta compañía y llamada *Civic Wallet*, que permite la integración del proceso de autenticación con el intercambio de criptomonedas en Ethereum o Bitcoins o incluso implementar otros procesos de autenticación utilizando la Civic Wallet como un mecanismo para autenticar un documento de identidad como la licencia de conducir o el pasaporte – muy similar al funcionamiento de ShoCard que utiliza un documento para comprobar la identidad del propietario y el esquema de almacenamiento de blockchain. En la ilustración 26, podemos apreciar el esquema general de funcionamiento del ecosistema de Identity Technologies [55].

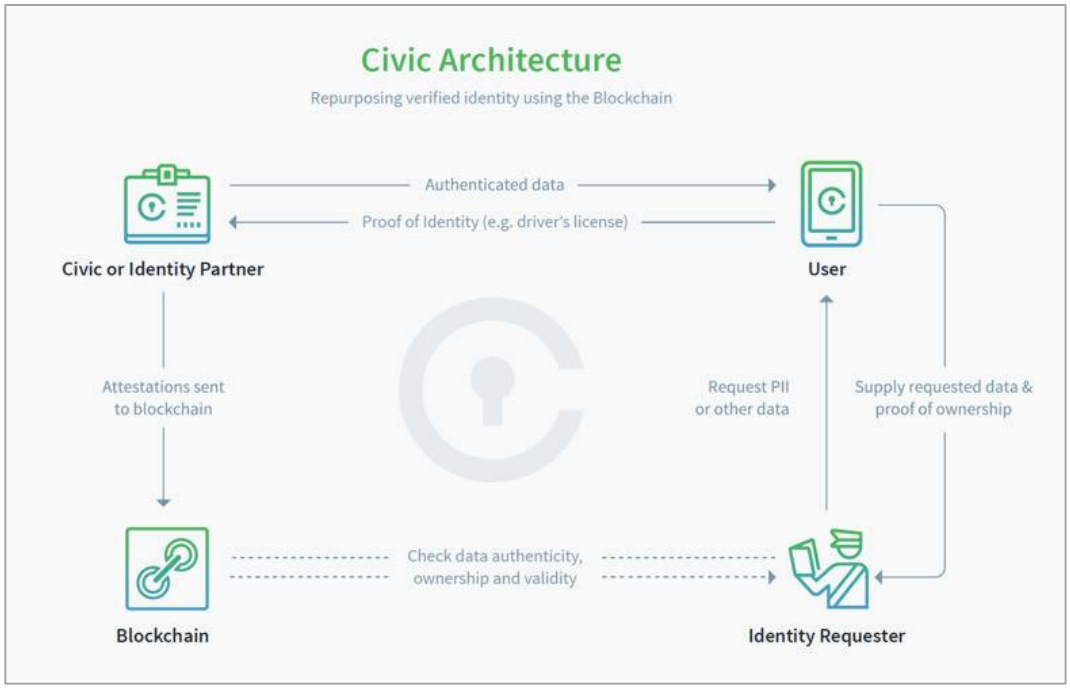

Ilustración 26 – Arquitectura de Civic. Identity Technologies [44].

Como se puede apreciar en el esquema anterior, el ecosistema está compuesto por 4 actores principales: La red de *blockchain* sobre la que corre la plataforma de servicios de Identity Technologies (denominados para efectos comerciales Identity.com), el *Identity requester* que puede ser un e-commerce o servicio web realizando un requerimiento de autenticación, el *User* o dueño de la identidad digital que se gestiona a través de la Civic Wallet y una parte independiente (para este caso a modo de ejemplo se seleccionó Onfido – proveedor de servicios de validación de autenticidad del registro biométrico o un documento de identidad del usuario) [44].

1.5.9 A cerca de blockchain en Colombia

En Colombia el desarrollo y comercialización de soluciones sobre blockchain se encuentra en una etapa temprana de exploración y desarrollo. El primer hackathon de blockchain de Colombia fue organizado por Mauricio Tovar de *ViveLab* en Bogotá, en octubre del 2017 (tan solo hace 3 años) y estuvo enfocado en la exploración de soluciones en cuatro sectores particulares: votaciones estudiantiles, comercio, salud y anti corrupción; el jurado compuesto por Lina Taborda, Directora de Políticas y Fortalecimiento de la Industria TI del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC); Sergio Martínez, Alto Consejero Distrital para las TIC de la Alcaldía Mayor de Bogotá; Iván Castaño, Gerente de Investigación, Desarrollo e Innovación también en el MINTIC, y el CEO de CriptoNoticias, Héctor Cárdenas, nos da un vistazo hacia los diferentes sectores público, privado y universitario que investigan en este campo [56].

Una mirada más amplia y actualizada sobre blockchain en el país la encontramos en el artículo "*Así va el negocio de blockchain en Colombia*" publicando en el 2019 en la revista Dinero [57], en éste

se indagan múltiples opiniones de expertos en la materia - explorando la visión actual de las universidades, equipos de investigación, la industria y el mismo gobierno; así como algunos retos que enfrenta esta naciente tecnología – cómo por ejemplo la falta de legislación. Así mismo se listan algunas iniciativas sobre blockchain como *Qubit Labs* - desarrollo liderado por Juan Carlos Marín y Lina Sánchez que ofrece una solución para la adquisición de boletas de eventos culturales, musicales y deportivos, usando la tecnología de bloques que permite enviar un código QR al celular y reemplazar la manilla o la boleta que utilizan los promotores de eventos tradicionales [58].

También resulta relevante el *Boletín Tecnológico - Blockchain* realizado en junio de 2018 por la Superintendencia de Industria y Comercio de Colombia, en el que se le presenta al sector financiero e industrial, una explicación de la tecnología, los avances en el país y las oportunidades que ofrece blockchain para la generación de nuevas formas de hacer negocios – destacando las soluciones que se vienen explorando por Coindex, Athenea, Criptobanco, Bitco y Minca - pequeñas o medianas empresas que se especializan en servicios financieros basados en blockchain [59].

Con relación a IdM sobre Blockchain en Colombia, el trabajo de investigación "*INFORME DE INVESTIGACIÓN: Mejoramiento de la seguridad de los servicios del Estado: verificación de identidad e integridad de documentos, a través de Blockchain*." desarrollado para el Centro de Innovación de Gobierno Digital del Ministerio TIC y la Universidad Distrital Francisco José de Caldas, explora la funcionalidad de Blockchain bajo el contexto colombiano utilizando la red *Ethereum* para verificar la validez y autenticidad de los documentos y las personas cuando se realicen trámites administrativos ante el Estado y de esta forma reducir a su mínima expresión el riesgo de falsificación de documentos mediante la inserción de estos en una cadena de bloques para que sean inalterables y conversen su integridad en la cadena administrativa [60].

1.5.10 Criptografía basada en identidad y control de acceso basado en atributos

Cómo hemos visto a lo largo del marco teórico y del estado del arte, el mundo de la identidad digital es profundo, cambiante y posee múltiples enfoques. Dos de ellos vale la pena mencionarlos debido a la cercanía con los retos de IdM – sin embargo no fueron incorporadas en el modelo propuesto debido a que no estaba en el alcance del presente trabajo y adicionalmente ambos enfoques pueden considerarse como capas complementarias de seguridad que podrían ser incorporadas al modelo propuesto si se llegaran a necesitar en otro trabajo de investigación y desarrollo futuro.

Criptografía basada en identidad o IBC

La criptografía basada en identidad o IBC por sus siglas en inglés (Identity Based Cryptography), consiste en utilizar alguno de los atributos de la identidad (como por ejemplo el correo electrónico, el número de identificación o incluso aspectos técnicos – como la dirección IP, para generar un cifrado de las comunicaciones, que no solo garantiza la confidencialidad de la información transmitida sobre una red), sino que además se convierte en sí misma en un mecanismo propio para validar la identidad del transmisor, pues utiliza dichos atributos como una semilla que inicializa el proceso de cifrado constituyéndose en una firma digital propia (Aunque cabe la aclaración no se

trata de utilizar la infraestructura de certificados digitales tradicionales tipo PKI, si se utiliza el modelo matemático de llaves privadas y públicas). El criptógrafo israelí Adi Shamir fue el pionero en proponer el modelo de IBC en 1998 en su paper "*Identity-based cryptosystems and signatures schemes*" [61]. A lo largo del tiempo, otros autores cómo Clifford Cocks [62] y Giuseppe Ateniese [63] entre otros, han propuesto mejoras y fortalecimiento sobre el modelo original de Shamir.

Control de accesos basados en atributos (ABAC)

Tradicionalmente en el proceso de interacción entre una persona y un sistema (o entre un sistema -sistema) se dan dos subprocesos: El subproceso de "autenticar" y el su proceso de "otorgar acceso" a los recursos; el subproceso de autenticar normalmente se presenta al inicio de la interacción y básicamente consiste en identificar quien es la persona o sistema con el cual se está interactuando, una vez se ha establecido la identidad, existe un conjunto de reglas o permisos específicos asociados a dicha identidad que le otorga acceso y privilegios de uso sobre ciertas partes de la información o incluso de la configuración del sistema – subproceso otorgar acceso; desde hace algunos años se ha venido fortaleciendo la seguridad en algunos sistemas de alta criticidad – complementando la autenticación del momento inicial con un grupo de reglas de negocio que permite cambiar los privilegios de uso evaluando en tiempo real algunas características específicas de la interacción entre las partes o atributos, a esto es a lo que llamamos Control de accesos basados en atributos (Attribute Based Access Control - ABAC).

Para explicar mejor este concepto podemos imaginar un escenario dónde Juan trabaja en el departamento de policía de su ciudad y tiene acceso a la base de datos de detenidos por este departamento de policía. Este acceso es un privilegio que está asociado a la identidad de Juan. Así que cuando él accede desde la red de datos local en las mismas instalaciones del departamento de policía tiene acceso de lectura, escritura e impresión a los registros de la base, igual ocurre cuando Juan ingresa a la base de datos desde su casa utilizando Internet. En un sistema basado en ABAC, uno de los atributos (para nuestro ejemplo tomaremos la dirección IP) es utilizado para ser evaluado al momento de otorgar acceso a Juan a la base de datos y ajustar dinámicamente los accesos de acuerdo al atributo, de forma que si está ingresando desde la red local, el sistema otorga acceso de lectura, escritura e impresión, pero si el acceso se está dando desde una red pública (la dirección IP es evaluada como un atributo que determina si el acceso es desde la red local o desde la red pública independiente de la identidad misma) se restringe el acceso de Juan a solo lectura de los registros. Así pues, el un sistema basado en ABAC, las reglas de acceso se aplican dinámicamente evaluando diferentes atributos para elevar los niveles de seguridad; esta forma de control de acceso está ampliamente detallada en la guía "*NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations*" [64].

1.6 Sistemas IdM utilizados por los 3 principales bancos del país

Ahora entonces se puede profundizar en el entendimiento de las soluciones IdM que cada uno de los bancos utiliza para la administración de identidades de sus clientes. Con el ánimo de salvaguardar la confidencialidad de los 3 bancos, se usaron códigos “Banco I”, “Banco II” y “Banco III” asignados aleatoriamente a cada banco estudiado.

1.6.1 Sistema de IdM Banco I

Banco I utiliza un modelo de IdM aislado, es decir que existe un único sistema de IdM y solo funciona para su portal de e-banking (lo que se denomina “solución de negocio”) – en consecuencia NO es compatible con ninguna otra solución de negocios. Además el banco es propietario de la identidad y de la información que se almacena en su sistema, aunque el usuario puede ingresar y cambiar las credenciales (cédula + contraseña) y una parte parcial de su información personal - una vez autenticado, no puede eliminar o manipular de ninguna otra forma su identidad.

Para obtener una identidad del sistema e-banking (o solución de negocio) el usuario primero debe ser cliente del banco abriendo un producto de su portafolio financiero, para ello debe acreditar su identidad física ante un funcionario del banco y de esta forma es el banco quien crea la identidad y posteriormente el usuario (cliente) puede ingresar al e-banking. Una vez creada la identidad se asigna un juego de credenciales para ingresar al portal (el número de la cédula de ciudadanía más una contraseña de entre 4 a 8 dígitos) que el mismo usuario crea por primera vez utilizando información adicional que solo el usuario y el banco posee (por ejemplo el número de cuenta de ahorros, o los últimos dígitos de su tarjeta de crédito, etc.). La contraseña es cifrada y transmite vía Internet hasta el host del banco para ser guardada (en forma de hash) y luego poder ser cotejada en futuras autenticaciones.

No fue posible encontrar información pública del modelo matemático utilizado por este banco en su sistema IdM para el almacenamiento de las credenciales ni el modelo matemático utilizado para autenticarlas. Cuando el usuario ingresa al sistema e-banking digitando su número de cédula y la contraseña, estas credenciales son transmitidas a través de internet utilizando el protocolo TLS 1.2 con llaves RSA 2084 y SHA 256, tal y como se muestra en la ilustración 27 a continuación.

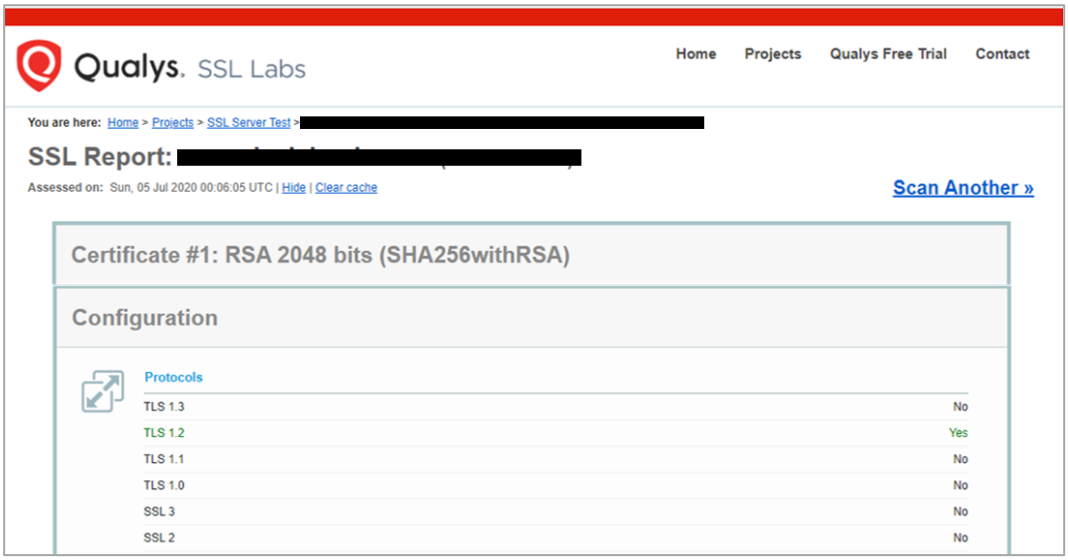

Ilustración 27 – Análisis de protocolos con Qualys al Banco I [65].

Para salvaguardar la seguridad de la identidad digital de sus clientes, el Banco I además utiliza un software especializado en protección de transacciones digitales bancarias que busca protección contra phishing y malware, requiriendo a sus clientes que descarguen e instalen el software en el dispositivo (computador o celular) desde el cual realizan transacciones bancarias en el e-banking.

Adicionalmente, el banco cuenta con un sistema de doble factor de autenticación utilizando un token que es requerido al realizar cierto tipo de operaciones en su portal de e-banking. Este token está vigente una única vez por un periodo de 3 minutos bajo el esquema OTP (One Time Password) y el usuario puede configurar el sistema IdM para enviar el token a su email o a su celular como un mensaje de texto (SMS).

1.6.2 Sistema de IdM Banco II

El Banco II cuenta con modelo de IdM aislado. Existe un único sistema de IdM que solo funciona para este portal de e-banking (o "solución de negocio") y NO es compatible con ninguna otra solución de negocios. El Banco II es propietario de la identidad y de la información que se almacena en su sistema, aunque igualmente, el usuario puede ingresar y cambiar sus credenciales (usuario + contraseña) y parte parcial de su información personal, pero no puede eliminar o manipular de ninguna otra forma su identidad.

Para obtener una identidad del sistema e-banking (o solución de negocio) el usuario primero debe abrir un producto del portafolio financiero de la entidad constituyéndose en "cliente", para ello debe acreditar su identidad física ante un funcionario del banco en sus instalaciones y luego asignar

una clave única para todos los productos que tenga en este banco (una aclaración, a pesar que el banco anuncia en medios la posibilidad de abrir cuentas y productos 100% desde Internet, a la fecha de este trabajo esta funcionalidad no estaba habilitada). Luego el banco crea la identidad en su propio sistema IdM con estos datos y almacena las credenciales internamente (NO fue posible encontrar información pública del modelo matemático utilizado por este banco en su sistema IdM para el almacenamiento de las credenciales ni el modelo matemático utilizado para autenticarlas).

Una vez creada la identidad al interior del banco, el usuario puede ingresar al portal de e-banking usando un juego de credenciales (número de cédula más la contraseña de 4 dígitos). Luego de ingresar la primera vez al portal, se le solicita al usuario crear un nombre de usuario o "nickname" - que a partir de este momento reemplazara el número de la cédula en sus credenciales-, adicionalmente deberá seleccionar una frase y una imagen de seguridad que será desplegada en el portal cada vez que el usuario ingrese al e-banking como un mecanismo adicional para prevenir casos de Phishing. La contraseña es cifrada y transmite vía Internet hasta el host del banco para ser guardada (en forma de hash) y luego poder ser cotejada en futuras autenticaciones. NO fue posible encontrar información pública del modelo matemático utilizado por este banco en su sistema IdM para el almacenamiento de las credenciales. Cuando el usuario ingresa al sistema e-banking digitando su nombre de usuario y contraseña las credenciales son transmitidas a través de internet utilizando el protocolo TLS 1.2 con llaves RSA 2084 y SHA 256, ver ilustración 28.

Adicionalmente, el banco cuenta con un sistema de doble factor de autenticación utilizando un token que es requerido al realizar algunas operaciones en su portal de e-banking. Este token está vigente una única vez por un periodo de 1 minuto bajo el esquema OTP (One Time Password) – el usuario puede configurar el sistema IdM para enviar el token a su email, a su celular como un mensaje de texto (SMS) o que sea desplegado en la App (aplicación móvil) del mismo banco.

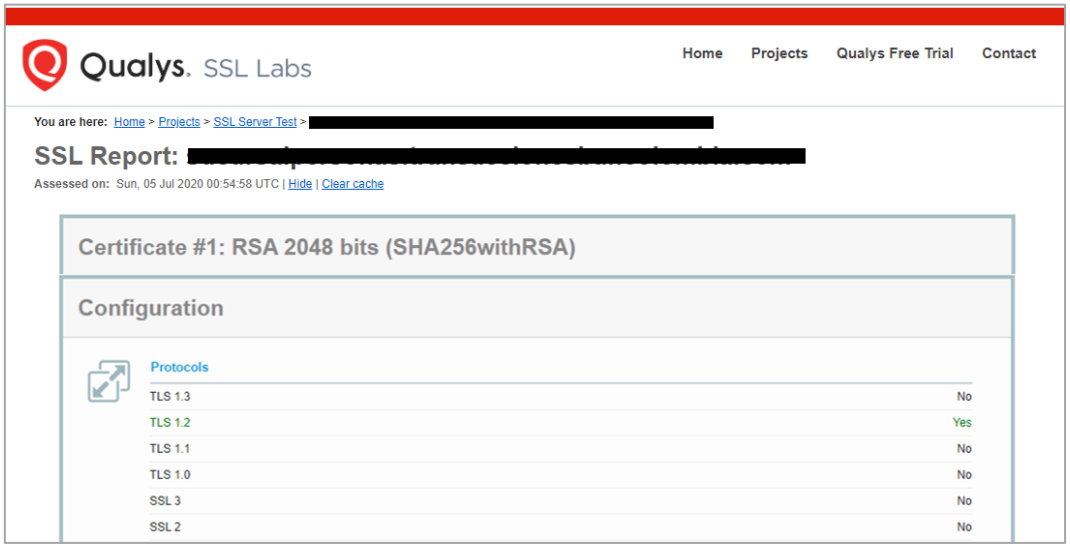

Ilustración 28 – Análisis de protocolos con Qualys al Banco II [65].

1.6.3 Sistema de IdM Banco III

El Banco III igual que los dos anteriores, maneja un modelo de IdM aislado. Posee un único sistema de IdM que maneja las identidades y no le sirve a ninguna otra solución de negocios. Esto hace que el banco sea el propietario de las identidades y por ende de toda la información que se almacena de éstas. El usuario puede ingresar y cambiar sus credenciales (cédula + contraseña) y también cambiar algunas variables de su información personal, pero no puede eliminar o manipular de ninguna otra forma su identidad.

Para obtener una identidad en el sistema de e-banking del Banco III, el usuario debe abrir un producto financiero de su portafolio, y tiene dos alternativas: acreditar su identidad física ante un funcionario del banco en las instalaciones del banco o siguiendo una serie de pasos en los que se valida su cédula y su cara a través de video por Internet. Una vez verificada la persona, el banco crea una identidad en su sistema de IdM y solicita al usuario generar una clave de mínimo 8 caracteres , así el banco crea la identidad y el hash de la contraseña en su propio sistema IdM, allí mismo guarda los datos adicionales de la identidad como email, dirección de residencia, etc. (NO fue posible encontrar información pública del modelo matemático utilizado por este banco en su sistema IdM para el almacenamiento de las credenciales ni el modelo matemático utilizado para cotejar las credenciales en la autenticación al momento de ingresar al e-banking). Cuando el usuario va a autenticarse, la contraseña es cifrada y transmite a través de Internet utilizando el protocolo TLS 1.2 con llaves RSA 2084 y SHA 256 – igual que los otros dos bancos analizados (ver ilustración 29). Adicionalmente este banco cuenta con un sistema de doble factor de autenticación utilizando un token que es requerido al realizar cierto tipo de operaciones en su portal de e-banking. Este token está vigente una única vez por un periodo de 1 minuto bajo el esquema OTP (One Time Password) – el usuario puede configurar el sistema IdM para enviar el token a su email, a su celular como un mensaje de texto (SMS) o que sea desplegado en la App (aplicación móvil) del mismo banco.

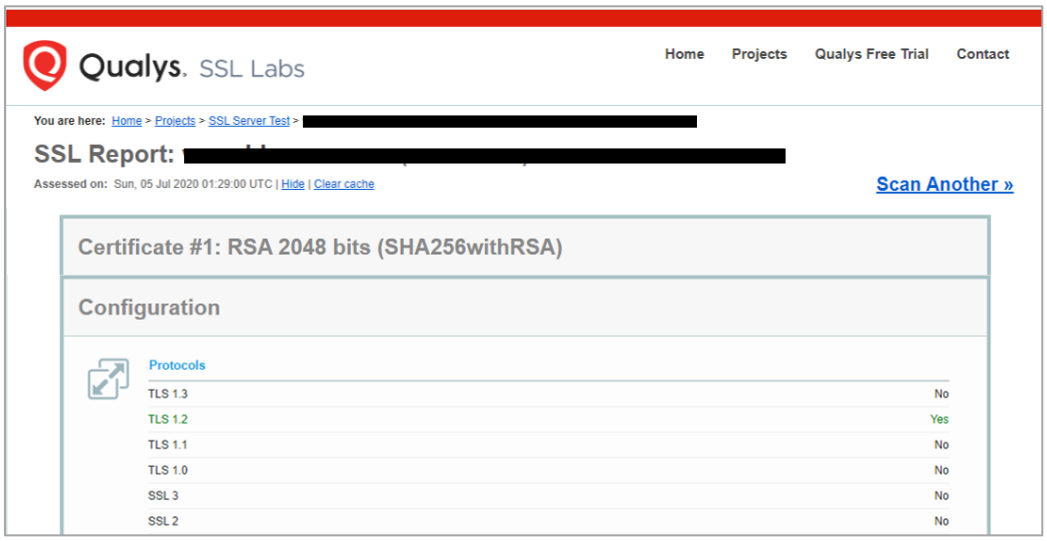

Ilustración 29 – Análisis de protocolos con Qualys al Banco III [65].

Información más detallada a cerca de los diferentes sistemas de IdM y los múltiples mecanismos de seguridad adicionales utilizados en la protección de la identidad de sus clientes por los bancos analizados, pueden consultarse las siguientes fuentes adicionales:

- Davivienda Elige solución de Easy Solutions Detect Safe Browsing [66].
- Apertura de cuenta online en BBVA Colombia [67]
- Portal transaccional de Bancolombia [68]
- Portal transaccional de BBVA [69]
- Portal transaccional de Davivienda [70].
- Demo sucursal virtual personas Bancolombia [71].
- Davivienda preguntas frecuentes [72].
- Aprender de seguridad en Bancolombia [73]
- Seguridad Davivienda [74].
- Seguridad digital en BBVA Colombia [75]
- Preguntas frecuentes Bancolombia [76]

2. Metodología

El presente trabajo fue realizado con el método deductivo, partiendo de lo general hasta llegar a lo específico y desarrollado en 4 grandes fases de acuerdo los objetivos trazados. En la ilustración 30 se presenta el esquema lógico de estas 4 fases.

Ilustración 30 – Fases metodológicas de la tesis.

Vale la pena mencionar que debido a los altos costos económicos, el tiempo y la complejidad tecnológica requerida para la implementación total de un modelo de IdM, no se utilizó una metodología experimental. La evaluación de efectividad del modelo propuesto estuvo soportada en la comparación de los niveles de vulnerabilidad a las técnicas de ataque de los 3 bancos analizados versus los niveles de vulnerabilidad del modelo propuesto.

A continuación se describen con mayor detalle, los pasos que fueron seguidos durante cada una de las fases.

2.1 Fase 1: Caracterizar las principales técnicas de robo de identidad

Para lograr caracterizar las principales técnicas de robo de identidad, se desarrollaron 6 pasos a saber:

Rastreo de información: Se realizó una identificación, lectura y clasificación de trabajos académicos asociados al robo de identidad, a las técnicas de ataque para robo de credenciales y a las investigaciones de brechas de seguridad de los últimos 5 años; utilizando para ello las siguientes bases de datos académicas: Scopus, IEEE, Google Académico y DirectScience; con un rango de búsqueda de 5 años (entre 2015 y 2020). Igualmente se amplió este rastreo de información a blogs, artículos e informes publicados en el mismo periodo de tiempo por empresas especializadas en seguridad informática como: Verizon, Symantec, McAfee, CheckPoint, Microsoft, entre otras. Finalmente se utilizó información de técnicas de ataque para robo de credenciales publicadas en organizaciones internacionales y referentes en ciberseguridad como NIST, INCIBE y MITRE.

Selección de fuentes: Una vez identificados y leídos los múltiples trabajos de investigación académicos, los diferentes blogs, informes, marcos de referencia y documentación técnica recolectada; fueron seleccionadas 7 fuentes de información y su correspondiente artículo o informe, que sirvieron de base para la consolidación de un listado único de las principales técnicas de ataque para el robo de credenciales. Estas 7 fuentes se seleccionaron en consideración a su detalle para describir las técnicas en sí mismas, la referencias hacia herramientas utilizadas para ejecutar los ataques y los resultados obtenidos ante el éxito de este.

Extracción de información: A continuación de cada fuente se extrajo un listado de las técnicas de ataque para el robo de identidad en forma de hoja de Excel, conservando el orden, los nombres y las subdivisiones utilizadas por la fuente.

Normalización de los datos: El paso siguiente fue retirar las subdivisiones usadas en cada fuente, de forma que se obtuviera un listado de técnicas de ataque en una única columna. A continuación se identificaron y eliminaron algunas técnicas de ataque que NO estaban directamente asociadas al robo de identidad (por ejemplo *Denegación de servicio o Hacking*), pues al entenderlas en profundidad, se pudo apreciar que no eran en sí mismas una técnica – como el caso de *Hacking* o que la técnica por sí misma no generaba el robo de identidad o de credenciales, cómo *Denegación de servicio*. Esta etapa generó una única lista, depurada y en formato de una columna con las técnicas de ataque listadas por cada fuente.

Consolidación: En este paso se unificaron en una sola hoja de Excel todas las técnicas normalizadas, colocando una columna por cada fuente. A continuación se unificaron los nombres, y se eliminaron de nuevo algunas técnicas duplicadas debido a la utilización de fuentes diferentes. El resultado final es un listado único consolidado con 25 técnicas de ataques usados para el robo de identidad digital, una descripción de la técnica en sí misma y la información que obtiene un atacante cuando logra ejecutarla exitosamente. En este punto cabe la claridad que las técnicas de robo de identidad son técnicas para el robo de credenciales, ya que las credenciales son las que le permiten al atacante materializar el robo de la identidad.

Caracterización: En este paso final de la FASE 1, se caracterizaron las diferentes técnicas de acuerdo con tres atributos: 1. *Contra quien va dirigida la técnica* (contra las personas o contra el sistema) – este atributo es importante porque al diseñar un modelo de IdM se utilizan mecanismos diferentes para proteger el sistema o las personas. 2. *Qué Información se obtiene con la técnica,* este atributo determina si el atacante logra obtener usuarios, contraseñas, hashes, cookies o tokens, o una combinación de algunos de estos factores de autenticación. Identificar las técnicas de ataque de acuerdo con la información que obtienen permite identificar - en un sistema IdM determinado - su nivel de vulnerabilidad a una técnica u otra. 3. *Etapa del proceso de IdM en la que se utiliza la técnica* – Esta caracterización se basa en las etapas del proceso de IdM planteadas en el numeral 3.2.1 y es importante, debido a que permite obtener mejores diseños de modelos de IdM conociendo y protegiéndose contra las técnicas de ataque que sufre la solución de IdM en cada una de las etapas del proceso.

En la ilustración 31, se muestra el esquema lógico de los pasos seguidos en la FASE 1.

Ilustración 31 – Pasos de la FASE 1.

El resultado final de la FASE 1, se presenta en la sección 3.1 con las principales técnicas de robo de identidad (Tabla 8) y la caracterización de dichas técnicas en la misma sección (Tabla 9). Igualmente, en el archivo de Excel "*Técnicas para el robo de identidad digital.xlsx*", adjunto en el presente trabajo, se encuentran el paso a paso y los resultados de la FASE 1.

2.2 Fase 2: Caracterizar las principales soluciones de IdM

Durante la FASE 2 se realizaron en 4 pasos descritos a continuación.

Identificación de modelos de IdM: Sabiendo que en el mercado actual existen cientos de soluciones de IdM y que cada día surgen nuevas, se hizo necesario entonces seleccionar un marco basado en "Modelos de IdM" que permitiera agrupar, caracterizar y entender las diferentes soluciones del mercado de acuerdo a atributos específicos. Para ello se realizó una identificación, lectura y clasificación de trabajos académicos asociados a modelos conceptuales de IdM y a las definiciones y características de una solución de administración de identidades, utilizando las bases de datos académicas Scopus, IEEE, Google Académico y DirectScience; con un rango de búsqueda de 5 años (entre 2015 y 2020). Igualmente se investigó el tema en blogs, artículos e informes publicados en el mismo periodo de tiempo por empresas especializadas en soluciones de identidad y accesos como Microsoft, IBM, Oracle, Gartner, entre otras. Luego de la identificación y lectura de

múltiples autores, se encontró convergencia en cuatro modelos de IdM específicos, que son presentados en detalle en la sección 1.3.4 del presente trabajo.

Documentación de las soluciones de IdM tradicionales: Como ya se mencionó, existe una gran cantidad de soluciones de IdM tradicionales - es decir, que no están basadas en blockchain – lo que hace casi imposible identificarlas y estudiarlas a todas; por esta razón, para el presente trabajo, se acotó el número de soluciones de IdM tomando como base la evaluación que realiza cada año la firma de consultoría Gartner y en la que se destacan las cinco soluciones de administración de identidades tradicionales más representativas del mercado, ubicadas en el "cuadrante mágico de Gartner de 2019". El estudio de estas soluciones permitió además la formulación de las *Etapas del proceso de IdM* (sección 3.2.1), fundamental a su vez para entender cómo y en que etapas del proceso se aplican las diferentes técnicas de robo de credenciales.

Documentación de las soluciones de IdM en blockchain: En este apartado, se profundizó en el entendimiento de blockchain: sus características, componentes tecnológicos y la forma en la que operan las nuevas soluciones que surgen a nivel mundial sobre esta arquitectura; para ello se realizó una identificación, lectura y clasificación de trabajos académicos y comerciales asociados a la tecnología de bloques; usando bases de datos académicas como Scopus, IEEE, Google Académico, DirectScience y algunos foros y blogs especializados en el tema - como el propio Bitcoin; con un rango de búsqueda de datos de 10 años (entre 2010 y 2020). Esta recopilación de información permitió identificar 4 de las principales soluciones de IdM sobre blockchain en el mercado actual y de acuerdo a los múltiples autores referenciados. Además sentó las bases para la propuesta del nuevo modelo de IdM sobre blockchain gracias al concepto de Identidad auto soberana – explicado en la sección 1.5.3 y que se convirtió en la piedra angular del nuevo modelo propuesto en el presente trabajo gracias a sus características: identidad manejada completamente por el usuario, agnóstica a los sistemas de e-banking y segura por sí misma.

Documentación de soluciones de IdM de los 3 principales bancos de Colombia: En este paso se realizó una investigación y documentación de los modelos de IdM que actualmente utilizan los 3 principales bancos de Colombia para administrar las identidades y el acceso de los clientes en sus portales de e-banking. Para lograr esto, se obtuvo información directamente de los portales de las entidades financieras, se revisó el código fuente público de estos portales y se recolectó información de fabricantes que operan detrás de dichas soluciones. Para salvaguardar la confidencialidad se asignó aleatoriamente un código a cada banco.

Caracterización: Se caracterizaron las soluciones de IdM con base al tipo de modelo de IdM que tienen y un conjunto de 15 características que representan mayor seguridad, transparencia, interconectividad y usabilidad de un sistema IdM de acuerdo con las leyes de la identidad y los modelos referenciados. Así se logró el cuadro de caracterización de los modelos IdM en la sección 3.2.3. En la ilustración 32, se aprecia un esquema conceptual de los pasos de la FASE 2.

Ilustración 32 – Pasos de la FASE 2.

El resultado final de la FASE 2 - disponible en la sección 3.2 - fue la "Caracterización de los sistemas IdM de los 3 principales bancos del país" y la propuesta del "Proceso de IdM y sus etapas básicas"

2.3 Fase 3: Construir un modelo teórico de IDM sobre blockchain

El camino recorrido en las FASES 1 y 2 sirvió de preparación para llegar a la FASE 3, aportando elementos cruciales en la construcción de la propuesta teórica del nuevo modelo de IdM sobre blockchain para e-Banking en Colombia. La fase 3 se enfocó entonces en la formulación del nuevo modelo.

Para la construcción del modelo se recogieron y potencializaron las condiciones ideales de un sistema de administración de identidades propuesta en las Leyes de la identidad, las principales características de seguridad ofrecidas por las soluciones de IdM a nivel comercial que fueron estudiadas, las técnicas de ataque para el robo de identidad y sus características y finalmente, las ventajas ofrecidas por blockchain a nivel de escalabilidad, seguridad, inmutabilidad, descentralización y transparencia.

El modelo fue construido bajo la mirada holística del proceso de IdM, incorporando elementos de seguridad en cada una de las etapas de dicho proceso y fortaleciendo los puntos vulnerables que atacan las principales técnicas usadas por los ciberdelincuentes para el robo de credenciales.

El resultado final de la FASE 3 fue la construcción y presentación del nuevo modelo de IdM sobre blockchain denominado *Modelo de IdM auto soberano con garante* presentado en la sección 3.3.

2.4 Fase 4: Comparar el modelo propuesto vs. modelos actuales

El propósito de la FASE 4 fue comparar las fortalezas y debilidades del modelo propuesto versus las soluciones de IdM analizadas y utilizadas por los 3 principales bancos del país. Para ello se utilizó una evaluación cuantitativa y una comparación cualitativa.

Para la evaluación cuantitativa se tomó la lista con las técnicas de ataque para el robo de identidad obtenida en la sección 3.1 y se analizó el nivel de vulnerabilidad a cada técnica que presentan los 4 modelos de IdM - los 3 que actualmente utilizan los bancos y el modelo propuesto. La forma de evaluar consistió en asignar un valor de "1" cuando la técnica de ataque puede afectar a la solución o modelo de IdM. Un valor de "0" si la técnica no lo afecta y un valor "S/D" que indica que no se

obtuvieron datos para realizar la evaluación correspondiente. De esta evaluación se obtuvo el puntaje de nivel de vulnerabilidad de cada una de las soluciones y el modelo propuesto de IdM.

La comparación cualitativa se realizó tomando las características idóneas de una solución de IdM que se presentaron en la sección 3.2.1 y se compararon igualmente contras los 4 modelos - los 3 que actualmente utilizan los bancos y el modelo propuesto. Pudiendo así responder con base en esta evaluación y en la comparación, la hipótesis de la cual se partió:

¿Un modelo teórico de administración de identidad digital (IdM) sobre blockchain podría ofrecer mayores fortalezas que los sistemas de IdM tradicionales (no blockchain), frente a la mitigación de riesgo por suplantación de identidad en sistemas de e-banking en Colombia? La respuesta se puede encontrar en las secciones 3.4 y 3.5

3. Resultados

3.1 Principales técnicas de robo de identidad digital

A continuación se presentan las principales técnicas de ataque utilizadas para el robo de credenciales y por ende para el robo de identidad digital. En la tabla 8 se encuentra una descripción de cada técnica y los factores de autenticación obtenidos por el atacante al ejecutarla exitosamente.

PRINCIPALES TÉCNICAS DE ATAQUE PARA EL ROBO DE IDENTIDAD		
TÉCNICAS DE ATAQUE (Para el robo de credenciales)	**DESCRIPCIÓN DE LA TÉCNICA**	**DATOS OBTENIDOS** (Ante el éxito de la técnica)
Brute force	Técnica de ataque en la que se intenta adivinar una clave probando todas sus combinaciones posibles hasta obtener la correcta.	Usuarios. Contraseñas.
Directory Traversal	Esta técnica explota la configuración de permisos en un sitio web, permitiéndole al atacante acceder a directorios superiores (padre) sin ningún control y acceder a información no autorizada.	Usuarios. Contraseñas.
DNS hijacking	En esta técnica un atacante controla y modifica un servidor DNS para que sus víctimas sean redireccionadas a sitios maliciosos (tipo phishing) y así poder obtener sus credenciales.	Usuarios. Contraseñas.
Sniffing	Técnica utilizada para escuchar todas las comunicaciones de datos dentro de una red (interna o pública), utilizando herramientas capaces de capturar y descomponer el tráfico de red de forma que se puede tener acceso a información sensible o confidencial.	Usuarios. Contraseñas. Cookies. Tokens.
Execution Code	Técnica con la que se aprovecha un programa mal escrito en su código fuente o vulnerable por su versión y se inyecta código en dicha aplicación, para que el sistema realice acciones no autorizadas.	Usuarios. Contraseñas. Cookies. Hashes. Tokens.
Exposed passwords	Corresponde a la utilización de credenciales adquiridas ilegalmente gracias a la exposición masiva de datos de una brecha de seguridad ocurrida en otro sistema.	Usuarios. Contraseñas.
Http Response Splitting	Técnica en la que se inyecta en los retornos de línea del protocolo HTTP para inyectar o alterar contenido del sitio web exponiendo información o induciendo al usuario a ver y ejecutar código malicioso.	Usuarios. Contraseñas. Cookies.
Leaked databases	Esta técnica consiste en la utilización de credenciales y otra información asociada a la identidad digital aprovechando la revelación de grandes bases de datos que fueron previamente hackeadas.	Usuarios. Contraseñas.
LSASS - Directory attack	Técnica de ataque enfocada en obtener las contraseñas cifradas de la base de datos de un servicio de directorio activo del tipo LDAP.	Usuarios. Contraseñas. Hashes.
Malware Banking trojans Webinjects	Troyano especializado en robar credenciales después de que éstas son desencriptadas y antes de ser mostradas por el browser.	Usuarios. Contraseñas.
Malware Keyloggers	Malware especializado en robar credenciales interceptando los comandos del teclado cuando el usuario está digitando su usuario y contraseña.	Usuarios. Contraseñas.
Malware Stealers	Malware especializado en el robo de información bancaria y de cualquier tipo de credenciales y datos de identificación que tenga el usuario en su dispositivo enviándolo a un servidor central.	Usuarios. Contraseñas. Tokens.

Man-in-the-Middle	Este ataque intercepta la comunicación entre dos sistemas conectándose en el medio de cada uno y haciéndose pasar por cada extremo, de forma que logra interceptar los mensajes que van cifrados.	Usuarios. Contraseñas. Cookies. Hashes. Tokens.
Memory Corruption	Esta técnica inyecta a un sistema a parámetro mal formados de modo que el sistema no sabe cómo manejarlo y entra en falla, entregando información o incluso el control del sistema al atacante	Usuarios. Contraseñas. Cookies. Hashes. Tokens.
Overflow	Esta técnica satura la capacidad de un sistema enviando el máximo de parámetros a alguno de sus componentes, forzando a un fallo del sistema que entrega información o incluso el control del mismo sistema.	Usuarios. Contraseñas. Cookies. Hashes. Tokens.
Pass-the-hash attack (PtH)	En esta técnica de ataque se capturan los hashes completos usados por los protocolos de autenticación (en especial Kerberos, NTLM o LanMan) y luego se reutilizan para suplantar al usuario	Hashes.
Phishing Real-time	Técnica basada en el phishing tradicional, pero se enfoca en obtener el token adicional al usuario y la contraseña y enviarlos al delincuente en tiempo real para ser utilizados por el atacante de inmediato.	Usuarios. Contraseñas. Tokens.
Phishing Traditional	Este ataque se basa en la utilización de un sitio web falso que solicita y captura las credenciales del usuario y luego las pasa al atacante.	Usuarios. Contraseñas.
Physical Keylogger	Dispositivo físico conectado entre el teclado y el computador para robar credenciales interceptando los comandos del teclado cuando el usuario está digitando su usuario y contraseña	Usuarios. Contraseñas.
Shoulder surfing	Esta técnica se enfoca en obtener usuarios y contraseñas simplemente mirando cuando el usuario las introduce. Literalmente: Espiar sobre el hombro	Usuarios. Contraseñas.
Smishing	Esta técnica se basa en enviar a la víctima un mensaje de texto (SMS) para inducirla a ingresar a un sitio falso (phishing) y capturar sus credenciales.	Usuarios. Contraseñas.
Social engineering	En general, es cualquier truco o actividad orientada a engañar a la víctima (ser humano), para que ella mismo entregue las credenciales.	Usuarios. Contraseñas. Tokens.
Sql Injection	Esta técnica consiste en inyectar sentencias de lenguaje SQL a sitios web que aceptan información a través de un formulario, pudiendo acceder a información sensible o incluso tener cierto nivel de acceso a la configuración del sistema.	Usuarios. Contraseñas. Hashes. Tokens.
Vishing	Esta técnica se basa en realizar una llamada telefónica fraudulenta induciendo a la víctima a decir sus credenciales.	Usuarios. Contraseñas.
XSS	El cross site scripting (XSS) se aprovecha de sitios web con código mal escrito o vulnerable que no ha sido corregido, forzando la ejecución de comandos en sitios cruzados. Esto se logra alterando los mensajes de comunicación que se le envían al servidor.	Usuarios. Contraseñas. Hashes. Tokens.

Tabla 8 – Principales técnicas de ataque para el robo de credenciales.

3.1.1 Caracterización de las técnicas de robo de identidad digital

Una vez consolidadas y entendidas las técnicas de ataque utilizadas para el robo de identidad digital, se caracterizaron de acuerdo con tres parámetros:

Etapa del proceso de IdM en la que se utiliza la técnica: Esta caracterización está basada en las Etapas del proceso de IdM planteadas en el numeral 3.2.1. Comprender en cuál de las etapas del

proceso de IdM se utiliza una técnica u otra nos permite proteger el sistema de estas debilidades desde el mismo diseño del modelo.

Contra quien va dirigida la técnica: En este punto, las técnicas se dividen en dos: técnicas usadas para atacar y obtener información sensible de las personas y las técnicas utilizadas para obtener información sensible directamente desde el sistema o la red de datos. Esta caracterización nos permite construir un diseño de modelo de IdM holístico que tenga en cuenta la protección de todos los actores (personas, red de datos y sistemas) que participan en la administración de la identidad.

Qué Información se obtiene con la técnica: Este atributo determina si el atacante logra obtener usuarios, contraseñas, hashes, cookies o tokens, o una combinación de algunos de estos factores de autenticación. Clasificar las técnicas por la información obtenida por el atacante, nos permite diseñar un modelo de IdM que minimice y/o proteja las credenciales contra las diferentes técnicas en forma integral.

A continuación se presenta la caracterización de las técnicas de robo de identidad en la tabla 9.

CARACTERIZACIÓN DE LAS TÉCNICAS DE ROBO DE IDENTIDAD DIGITAL			
TÉCNICAS DE ATAQUE (Para el robo de credenciales)	**ETAPA DEL PROCESO DE IdM** (que vulnera la técnica)	**TÉCNICA DIRIGIDA CONTRA**	**DATOS OBTENIDOS** (Ante el éxito de la técnica)
Brute force	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
Directory Traversal	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
DNS hijacking	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
Sniffing	Intercambio de credenciales	El sistema	Usuarios, Contraseñas, Cookies, Tokens
Execution Code	Almacenamiento, Intercambio de credenciales, Autenticación, Otorgamiento de accesos	El sistema	Usuarios, Contraseñas, Cookies, Hashes, Tokens
Exposed passwords	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
Http Response Splitting	Almacenamiento, intercambio de credenciales	El sistema	Usuarios, Contraseñas, Cookies
Leaked databases	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
LSASS - Directory attack	Autenticación	El sistema	Usuarios, Contraseñas, Hashes
Malware Banking trojans Webinjects	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
Malware Keyloggers	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
Malware Stealers	Almacenamiento, intercambio de credenciales	El sistema	Usuarios, Contraseñas, Tokens
Man-in-the-Middle	Intercambio de credenciales	El sistema	Usuarios, Contraseñas, Cookies, Hashes, Tokens
Memory Corruption	Almacenamiento, Autenticación	El sistema	Usuarios, Contraseñas, Cookies, Hashes, Tokens
Overflow	Almacenamiento, Autenticación	El sistema	Usuarios, Contraseñas, Cookies, Hashes, Tokens
Pass-the-hash attack (PtH)	Intercambio de credenciales	El sistema	Hashes
Phishing Real-time	Intercambio de credenciales	La persona y el sistema	Usuarios, Contraseñas, Tokens
Phishing Traditional	Intercambio de credenciales	La persona y el sistema	Usuarios, Contraseñas

Physical Keylogger	Intercambio de credenciales	El sistema	Usuarios, Contraseñas
Shoulder surfing	Intercambio de credenciales	La persona	Usuarios, Contraseñas
Smishing	Intercambio de credenciales	La persona	Usuarios, Contraseñas
Social engineering	Intercambio de credenciales	La persona	Usuarios, Contraseñas, Tokens
Sql Injection	Almacenamiento, Autenticación	El sistema	Usuarios, Contraseñas, Hashes, Tokens
Vishing	Intercambio de credenciales	La persona	Usuarios, Contraseñas
XSS	Almacenamiento, Autenticación	El sistema	Usuarios, Contraseñas, Hashes, Tokens

Tabla 9 – Caracterización de las técnicas de robo de identidad.

Esta caracterización es una de las bases para la formulación del nuevo modelo de IdM sobre blockchain, permitiendo reforzar la protección de credenciales, la intervención de las personas cada una de las etapas del proceso mismo.

3.2 Caracterización de las principales soluciones de IdM

Para caracterizar las soluciones de IdM de los 3 principales bancos de Colombia, se tomaron en cuenta las condiciones idóneas propuestas en las Leyes de la Identidad de Kim Cameron y las condiciones idóneas encontradas en el análisis de solución de IdM actuales (tradicionales y sobre blockchain), estableciendo así una lista de 15 atributos o características con las que se puede tipificar una solución de IdM. La descripción de estas características las encontramos en la tabla 10, a continuación.

CARACTERIZACIÓN DE LAS PRINCIPALES SOLUCIONES DE IDM	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Tipo de Modelo de IdM.	Permite identificar rápidamente la arquitectura y la filosofía de la solución de IdM analizada.
El sistema IdM permite que el dueño de la identidad sea el usuario.	Permite conocer si el control sobre los datos y el uso de la información está en manos del dueño de la identidad o del administrador del sistema IdM.
El sistema IdM verifica la identidad real de la persona que crea la identidad.	Esta característica es esencial para los sistemas e-banking ya que permite el cumplimiento de la regulación sobre conocimiento del cliente y evita suplantación desde la etapa de enrolamiento.
El sistema IdM revela información solo con el consentimiento del usuario.	Esta característica identifica si el dueño de la identidad tiene el control al momento de ser utilizada su identidad o la información que ella almacena, protegiéndolo de usos no autorizados en los casos en los cuales un atacante puede tener acceso a sus credenciales o incluso ante eventos en los que se vulnera algún sistema en el que se guardaron sus datos.
El sistema IdM almacena la información mínima posible.	Esta condición hace referencia al diseño mismo del sistema de IdM y pone énfasis en utilizar y por ende exponer el mínimo de información de una identidad en las diferentes interacciones, reduciendo el impacto ante una vulneración del sistema de IdM mismo.
El sistema IdM distribuye el almacenamiento de las identidades.	Identifica si la solución de IdM tiene un esquema de almacenamiento de las identidades centralizado o distribuido, haciéndolo más o menos vulnerable ante hackeo al mismo sistema.
El sistema IdM permite al usuario eliminar o renovar la identidad.	Esta característica otorga control al usuario sobre la identidad misma y los datos almacenados en ella, sin necesidad de pasar por intermediarios.

El sistema IdM conserva evidencias y trazabilidad de acciones.	La información de quien utiliza la identidad, en que momentos, contra que sistemas y cuales datos de la identidad son compartidos, es visible para los diferentes actores.
El sistema IdM generar confianza previniendo engaños al usuario.	El diseño del sistema mismo evita suplantación entre las personas y/o los componentes tecnológicos que lo utilizan.
El sistema IdM ofrece protocolos y tecnologías abiertas sobre su funcionamiento.	El modelo de IdM, la tecnología, protocolos y estándares de cifrado utilizados en la solución de IdM son públicos y las diferentes partes involucradas pueden consultarlos sin restricción.
El sistema IdM es compatible, amigable e intuitivo para los humanos.	La manera en que el usuario final interactúa con el sistema de IdM es fácil de utilizar y no requiere un esfuerzo poco natural por parte del ser humano.
El sistema IdM protege las credenciales enviadas sobre una red de datos.	El intercambio de información de autenticación está protegido contra interceptaciones o alteraciones en la red de datos.
El sistema verifica la fuente de la que está recibiendo credenciales.	El diseño del sistema de IdM autentica igualmente al dispositivo desde el cual se recibe información.
El sistema utiliza un modelo matemático público de comparación de credenciales.	El o los algoritmos de comparación y autenticación de credenciales son públicos y abiertos para ser consultados por las partes sin restricción.
El sistema IdM protege su mensajería, evitando que pueda ser suplantada o alterada.	El intercambio de información está protegido contra interceptaciones o alteraciones o suplantación en la red de datos.

Tabla 10 – Características de los sistemas IdM.

3.2.1 Caracterización de los sistemas IdM de los 3 principales bancos del país

En la Tabla 11 se presenta entonces, la caracterización de los sistemas de IdM de los 3 principales bancos en Colombia.

CARACTERIZACIÓN DE LOS SISTEMAS IDM DE LOS 3 PRINCIPALES BANCOS DE COLOMBIA			
CARACTERÍSTICAS	**BANCO I**	**BANCO II**	**BANCO III**
Tipo de Modelo de IdM.	AISLADO	AISLADO	AISLADO
El sistema IdM permite que el dueño de la identidad sea el usuario.	NO	NO	NO
El sistema IdM verifica la identidad real de la persona que crea la identidad.	SI	SI	SI
El sistema IdM revela información solo con el consentimiento del usuario.	NO	NO	NO
El sistema IdM almacena la información mínima posible.	NO	NO	NO
El sistema IdM distribuye el almacenamiento de las identidades.	NO	NO	NO
El sistema IdM permite al usuario eliminar o renovar la identidad.	NO	NO	NO
El sistema IdM conserva evidencias y trazabilidad de acciones.	SI	SI	SI
El sistema IdM generar confianza previniendo engaños al usuario.	PARCIALMENTE	PARCIALMENTE	PARCIALMENTE
El sistema IdM ofrece protocolos y tecnologías abiertas sobre su funcionamiento.	PARCIALMENTE	PARCIALMENTE	PARCIALMENTE
El sistema IdM es compatible, amigable e intuitivo para los humanos.	SI	SI	SI
El sistema IdM protege las credenciales enviadas sobre una red de datos.	SI	SI	SI

El sistema verifica la fuente de la que está recibiendo credenciales.	NO	NO	NO
El sistema utiliza un modelo matemático público de comparación de credenciales	NO	NO	NO
El sistema IdM protege su mensajería, evitando que pueda ser suplantada o alterada.	SI	SI	SI

Tabla 11 – Caracterización de los sistemas IdM de los bancos y del modelo propuesto.

3.2.2 Definición del proceso de IdM y sus etapas básicas

Para construir un nuevo Modelo de IdM basado en blockchain, fue necesario la formulación de un enfoque sistémico y de proceso para la administración de identidades. La definición del proceso y sus etapas permitió identificar puntos débiles en cada etapa y tenerlos en cuenta al construir la propuesta del nuevo modelo de IdM. En la ilustración 33, se presentan las etapas básicas de un *Proceso de IdM.*

Ilustración 33 – Etapas básicas del proceso de IdM.

A continuación se describen las etapas del proceso, identificando sus principales retos a nivel de seguridad.

Creación de la identidad: También conocida como Onboarding, en esta etapa se crea la identidad en el sistema IdM respectivo, se recolectan los datos de información asociados a la identidad misma (por ejemplo correo electrónico, número de identificación personal, fecha de nacimiento, dirección, etc.) y se generan las credenciales. Entre los principales retos durante esta etapa del proceso se tienen: evitar la creación de falsas identidades (particularmente en sistemas e-banking) y evitar que el primer juego de credenciales caiga en manos equivocadas.

Almacenamiento de la identidad: Durante esta etapa, el sistema IdM guarda la identidad, la información asociada a la misma y un enlace a las credenciales generadas en la etapa 1, de forma que se pueda utilizar más adelante durante la autenticación - creando así un vínculo entre las credenciales y la identidad. Uno de los mayores retos frente al robo de identidad en esta etapa es el mecanismo técnico seleccionado para almacenar las credenciales y la información de la

identidad, pues ante un hackeo del sistema esta información podría ser tomada por el delincuente, vulnerando a todos los usuarios de dicho sistema IdM.

Intercambio de Credenciales: Es en esta etapa dónde el usuario envía sus credenciales al sistema con el que va a interactuar (normalmente usuario + contraseña, pero pueden ser otros elementos como llaves públicas, factores biométricos, token, etc.). En esta etapa se tienen dos grandes retos para garantizar la seguridad: como enviar credenciales que no sean "interceptadas" en el camino y como garantizar que las credenciales que está recibiendo el sistema si las está enviando realmente el dueño de la identidad.

Autenticación: Es en este punto dónde el sistema de IdM recibe las credenciales y las coteja (normalmente a través de un comparativo matemático) para validar si son correctas o no, retornando un mensaje de autenticación correcta o incorrecta respectivamente. La fortaleza matemática del sistema de validación de las credenciales es uno de los retos más grandes en este punto para lograr un equilibrio entre la seguridad y la experiencia del usuario.

Otorgamiento de accesos: En esta etapa final, si la autenticación de credenciales fue aprobada, el sistema IdM retorna un mensaje exitoso a la solución para que ésta pueda otorgar accesos a la identidad acorde con su lógica de negocio. El reto mayor en esta etapa es evitar la suplantación del mensaje de autenticación exitosa que pudiera engañar a la solución de negocio.

3.3 Construcción de un modelo de IdM sobre blockchain

3.3.1 Ampliación de los modelos actuales de IdM

Luego de recorrer múltiples investigaciones, modelos y soluciones de IdM y de profundizar en el funcionamiento y la filosofía de las soluciones actuales, fue necesario ampliar la conceptualización de los modelos de IdM existentes a la fecha, proponiendo la creación de un nuevo modelo de IdM que aproveche las ventajas de blockchain, mejore la seguridad y simplifique la experiencia de los actores del sistema. En la ilustración 34 presentamos la propuesta del nuevo modelo .

Ilustración 34 – Ampliación de los modelos de IdM referenciados.

3.3.2 Nuevo modelo de IdM auto soberano con garante

El nuevo modelo está basado en el concepto de "auto identidad soberana", explicado previamente en la sección 1.5.3 incorporando además un elemento vital: "el garante" que verifica la coherencia entre la identidad digital y la identidad real de la persona. El rol de garante en Colombia lo ejercerían las notarías, responsables entonces de verificar y garantizar que la identidad digital que se está creando corresponde con la identidad física del solicitante. Este proceso es similar al que hoy realizan las notarías para la autenticación de documentos físicos garantizando que quién lo firmó sea la persona real. La ilustración 35 a continuación, nos permitirá visualizar los diferentes pasos y actores que intervienen en este nuevo modelo de IdM auto soberano con garante.

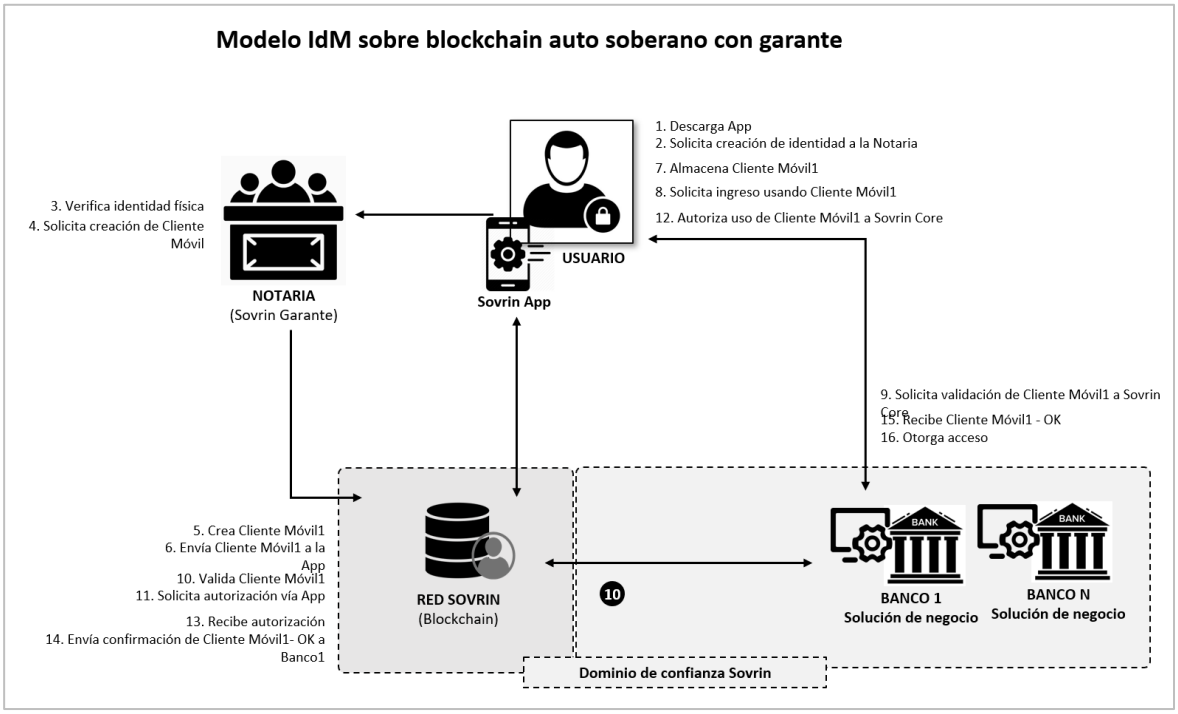

Ilustración 35 – Modelo propuesto de IdM AUTO SOBERANO CON GARANTE

Como se puede apreciar en la ilustración 35, el usuario inicia el proceso descargando la App de Sovrin(1), y se dirige a una notaría para solicitar la creación de la identidad digital (2), la notaria constata su documento de identidad y registro biométrico (3) y diligencia la información de la identidad del usuario enviando la solicitud de creación a la red de Sovrin (4). La red crea la identidad en formato SovrinID (5) y se la envía a la App del usuario (6) dónde es almacenada (7).

Cuando el usuario desea ingresar al e-banking de la entidad financiera lo hace utilizando su SovrinID (8), el banco la recibe y la reenvía a la red de Sovrin para su validación (9), Sovrin verifica la identidad (10) y le solicita al usuario en su App una autorización para utilizar dicha identificación contra el Banco (11).

El usuario Autoriza esta utilización de su identidad (12) y el mensaje es recibido por la red Sovrin (13), quien ahora envía un mensaje hacia el banco indicando que la SovrinID está OK (14). El banco

finalmente recibe la confirmación de que la identidad está bien (15) y otorga los accesos correspondientes (16).

Enrolamiento en el nuevo modelo

La etapa de enrolamiento o también llamada Onboarding, es particularmente importante, pues en ella es dónde se incorpora la nueva figura de garante – desempeñada por las notarías del país y se garantiza la coherencia entre la identidad digital y la identidad física. En la ilustración 36 se muestra en detalle el proceso de creación de la Identidad por primera vez en el nuevo modelo.

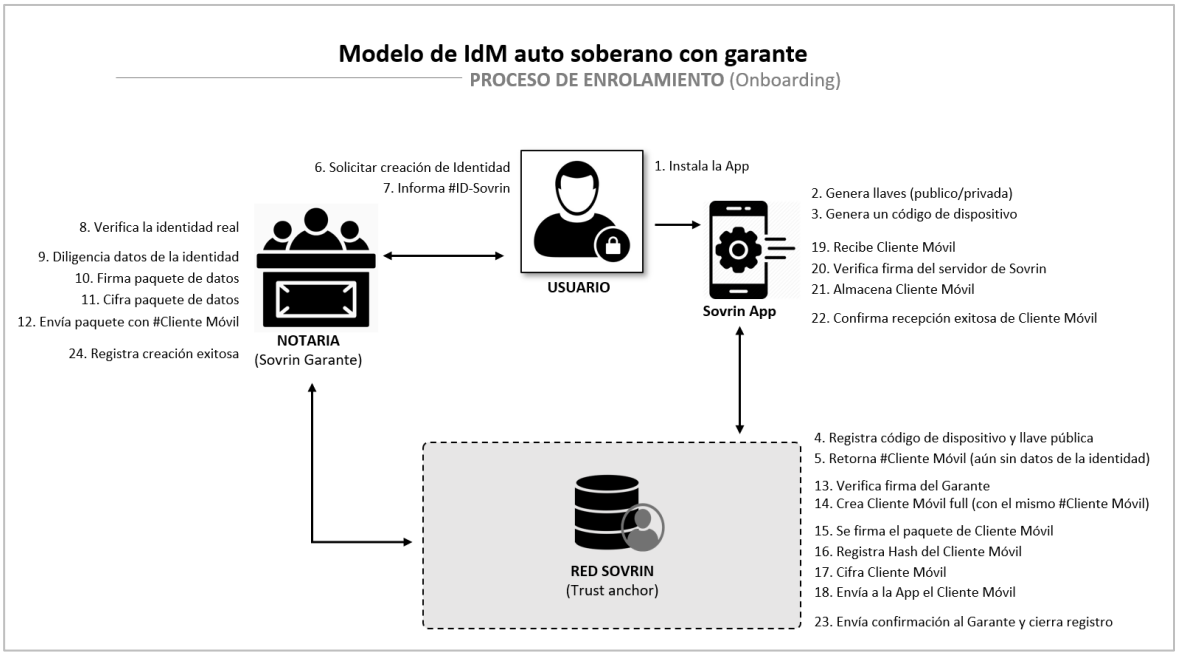

Ilustración 36 – Modelo de enrolamiento en IdM AUTO SOBERANO CON GARANTE

El Onboarding o proceso de enrolamiento inicia cuando el usuario descarga la App (puede ser en su dispositivo (móvil o en forma opcional en su computador) (1), al abrir la App por primera vez se le solicita autorización para crear un juego nuevo de llaves (publica/privada) que genera en forma automática la misma aplicación utilizando DPKI (Decentralized Public Key Infrastructure)(2). Una vez generado el juego de llaves, se crea un identificador único de dispositivo utilizando DIDs (Decentralized Identifiers)(3). De esta forma, la App se registra por primera vez en la red de Sovrin con su código de dispositivo y entrega su llave pública, que es almacenada en la red central y asociada por ahora al código del dispositivo (4), es en este momento que la red Sovrin genera un espacio de almacenamiento y un código de identidad en Sovrin -aunque por ahora está vacío, se identifica con código (#SovrinID) y no tiene aún información más que una llave pública y un código de dispositivo.

Este número – SovrinID - es cifrado con la llave pública del usuario y enviado a la App(5) a través de internet. Todo esto ocurre en segundos durante el primer contacto del usuario con la App y

finalmente al usuario se le despliega un mensaje invitándolo a que se desplace a la notaría más cercana para concluir con la creación de la identidad digital en Sovrin. Una vez el usuario se encuentra en la notaría, solicita la creación de una identidad digital en Sovrin (6) y entrega el correspondiente #SovrinID que es desplegado en la misma App (7).

La notaria recibe el #SovrinID y solicita el documento de identidad de la persona, validando su cédula (o equivalente) y verificando además el registro biométrico de las huellas (de acuerdo al procedimiento estándar para verificación de identidad física de las notarías)(8). De esta forma se convierte en garante de que la identidad digital que se va a crear en efecto corresponde a la persona correcta. Una vez se ha validad la identidad física, el funcionario de la notaria ingresa su aplicativo Sovrin y llena los datos requeridos para la creación de la identidad (9), al finalizar de diligenciar los datos los firmar con la llave pública de la notaría (10) y los cifra con la llave pública del servidor de Core al que se está conectando (11) para finalmente enviar esta solicitud (12).

En el Core de Sovrin se recibe esta solicitud y se verifica la firma digital de la notaria (13), se llenan los campos de la identidad (es toda la información que le llegó desde la Notaria) creando de esta forma un paquete completo de datos que se constituye entonces en la SovrinID (14). El paquete de datos con la SovrinID es firmado digitalmente por el servidor de Core con su llave pública (15) y además se genera un hash del paquete - para garantizar la inalterabilidad del mismo (16) y para dejar este hash en los registros del Core de Sovrin (Esto significa que la red Core de Sovrin no se guarda la identidad y sus datos, solo almacena en el libro mayor o DLT los siguientes datos: #SovrinID, código de dispositivo, llave pública, fecha de creación y registro de la notaría que lo garantiza y finalmente el hash del paquete de SovrinID). Una vez el paquete está listo, el servidor de la red de Sovrin lo cifra con la llave pública del usuario (17) y se lo envía a la App (18). Cuando le llega a la App (19), se verifica contra la llave pública del servidor de Core la respectiva firma del paquete (20) se almacena en forma exitosa la identidad en la App (21) y la App retorna un mensaje de recepción éxitos del paquete con la SovrinID al servidor de Core (22), Con este mensaje, el servidor de Core confirma a la notaría que todo fue exitoso. Finalmente envía una confirmación de éxito al Garante (23) y cierra el proceso.

3.3.3 Arquitectura del modelo IdM auto soberano con garante

Ahora veremos la arquitectura de blockchain sobre la que corre el presente modelo y que se agrupa en tres capas:

Capa de usuarios e instituciones: En ella se ubican las soluciones de negocio – para nuestro caso portales de e-banking de los diferentes bancos en Colombia y las aplicaciones móviles que utilizan los usuarios finales como dueños de la identidad - comunicándose a través de los protocolos abiertos, públicos y de uso libre que ofrece la red de blockchain, permitiendo así una fácil integración entre los portales de los bancos, los clientes móviles y la red de la solución de IdM en blockchain, igualmente en esta capa tenemos los usuarios (clientes actuales o potenciales de los bancos), que descargan y utilizan desde la App su identidad de la solución de IdM en blockchain interactuando con los portales de e-banking. Esta capa está protegida por la utilización de

certificados digitales descentralizados para el cifrado y firmado de las transacciones garantizando así la confidencialidad y la integridad y correo en forma distribuida asegurando la disponibilidad del ecosistema.

Capa de TRUST ANCHOR: En esta capa encontramos los servidores de las instituciones de confianza que hacen parte de la red de la solución de IdM en blockchain. Éstos son los únicos que pueden hacer el enrolamiento de clientes creando nuevas identidades y actualizando el libro mayor DLT que se custodia en la siguiente capa, sirviendo como garantes para la creación de las identidades. Esta capa igualmente está protegida por la utilización de certificados digitales descentralizados para el cifrado y firmado de las transacciones garantizando así la confidencialidad y la integridad y correo en forma distribuida asegurando la disponibilidad del ecosistema.

Capa de CORE: En esta capa se encuentran los servidores fundacionales de la solución de IdM en blockchain y los principales servidores donde se custodia la integridad y consistencia matemática del libro mayor y de las reglas de funcionamiento del modelo de IdM Auto soberano con Garante. En esta capa igualmente es dónde se hace el registro y la aceptación de los servidores que cumplirán con el rol de TRUST ANCHOR. A continuación se presenta la ilustración 37 con la arquitectura del modelo de IdM auto soberano con garante.

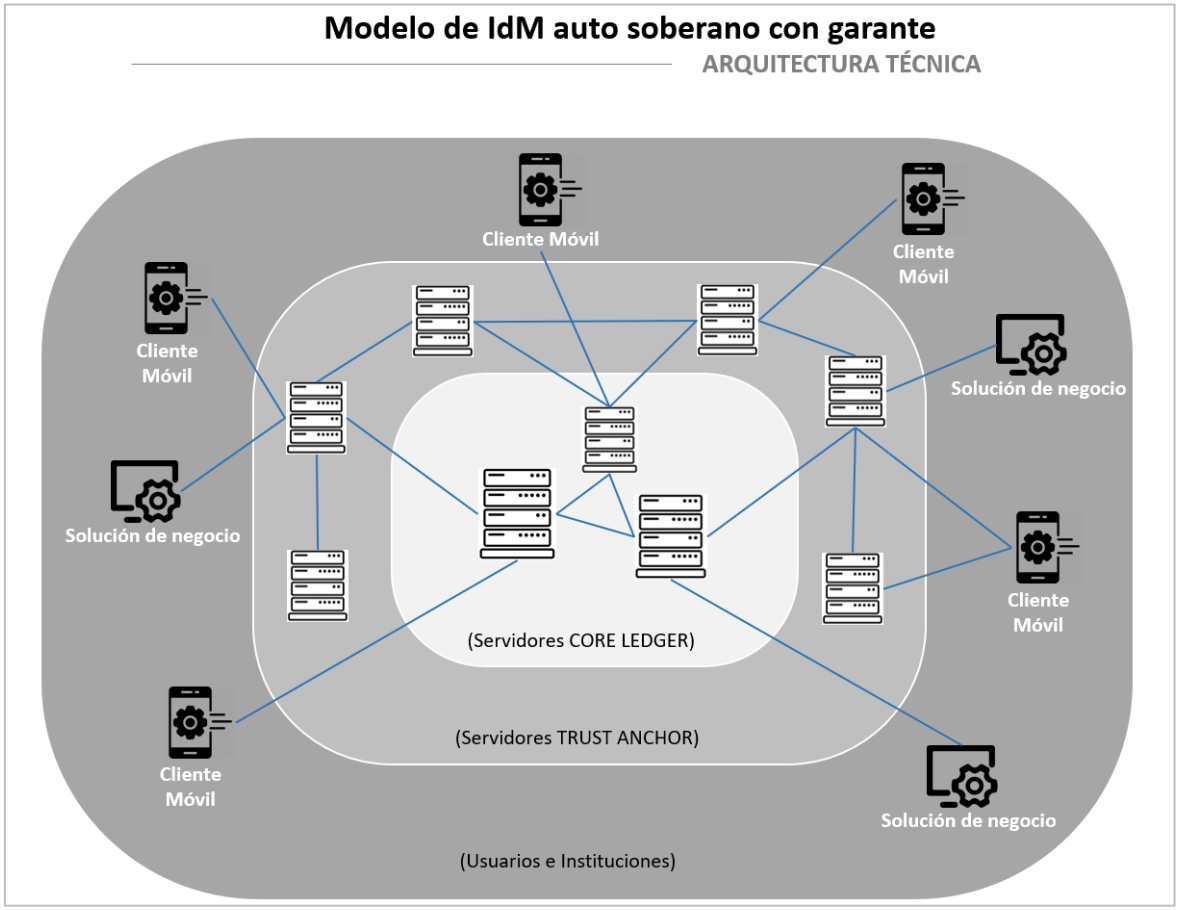

Ilustración 37 – Arquitectura técnica del modelo de IdM auto soberano con garante.

La capa de Core, al igual que sus dos capas anteriores, igualmente está protegida por la utilización de certificados digitales descentralizados para el cifrado y firmado de las transacciones garantizando así la confidencialidad y la integridad y correo en forma distribuida en estructura de red peer to peer, asegurando la disponibilidad del ecosistema.

Nota: Se seleccionó la plataforma Sovrin como base para este modelo, considerando tres razones: Ya incluye en su arquitectura el rol de "Trust anchor" lo que permite la adaptación del rol "garante" sin necesidad de grandes cambios tecnológicos. Sovrin continúa siendo una solución sin ánimo de lucro permitiendo libre acceso a sus recursos y finalmente cuenta con un sólido despliegue a nivel mundial, ofreciendo así una mayor escalabilidad y seguridad.

A continuación se realiza un cuadro comparativo con las ventajas de utilizar Sovrin como base del modelo auto soberano con garante, en la tabla 12.

COMPARATIVO ENTRE SOLUCIONES DE IdM SOBRE BLOCKCHAIN				
CAPACIDAD	**U-PORT**	**SOVRIN**	**SHOCARD**	**CIVIC**
Enrolamiento de identidades a través de terceros de confianza	NO	SI	NO	NO
Información y código abierto y de libre acceso	SI	SI	NO	SI
Despliegue estable a nivel global	SI	SI	NO	SI

Tabla 12 – Comparación entre las soluciones de IdM analizadas.

3.3.4 Valoración de seguridad del nuevo modelo vs. las técnicas de ataque

Luego de formular el modelo y de describir sus diferentes características y funcionamiento, a continuación se presenta una tabla en la que se analiza el nivel de vulnerabilidad del nuevo modelo de IdM auto soberano con garante versus las técnicas de ataque para el robo de identidad. La tabla 13 nos muestra los resultados de la evaluación, teniendo en consideración estas convenciones: "0" significa que NO es vulnerable a la técnica; "1" significa que SI es vulnerable a la técnica y "S/D" significa Sin datos para verificar si es o no vulnerable a la técnica.

VALORACIÓN DEL MODELO PROPUESTO vs. LAS TÉCNICAS DE ATAQUE			
TÉCNICA DE ATAQUE (Para el robo de credenciales)	**RESULTADOS (Ante el éxito de la técnica)**	**Nivel de vulnerabilidad del Modelo de IdM Auto soberano con garante**	**ANÁLISIS**
Brute force	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
Directory Traversal	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
DNS hijacking	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
Sniffing	Usuarios, Contraseñas, Cookies, Tokens	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **firma y cifra bidireccionalmente las cookies**, aunque se intercepten no le sirven al atacante. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado.
Execution Code	Usuarios, Contraseñas, Cookies, Hashes, Tokens	1	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **firma y cifra bidireccionalmente las cookies**, aunque se intercepten no le sirven al atacante. El modelo firma y cifra bidireccional los hashes, sin embargo la manipulación directa de la CPU **podría comprometer los Hashes** del sistema, haciendo vulnerable el modelo. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado.
Exposed passwords	Usuarios, Contraseñas	0	El modelo de IdM Auto soberano con garante **NO utiliza usuario ni contraseña**, autentica usando mensajería basada en llaves pública/privada
Http Response Splitting	Usuarios, Contraseñas, Cookies	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **firma y cifra bidireccionalmente las cookies**, aunque se capturen no le sirven al atacante.
Leaked databases	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **firma y cifra bidireccionalmente las cookies**, aunque se capturen no le sirven al atacante.
LSASS - Directory attack	Usuarios, Contraseñas, Hashes	S/D	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. No se cuenta con información para validar la vulnerabilidad a nivel de **los hashes** del sistema ante esta técnica de ataque.

Malware Banking trojans Webfilters	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
Malware Keyloggers	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
Malware Stealers	Usuarios, Contraseñas, Tokens	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado.
Man-in-the-Middle	Usuarios, Contraseñas, Cookies, Hashes, Tokens	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **firma y cifra bidireccionalmente las cookies**, aunque se intercepten no le sirven al atacante. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado. **El modelo firma y cifra bidireccional los hashes**. Al atacar los datos de red no se **podrían comprometer los hashes** del sistema.
Memory Corruption	Usuarios, Contraseñas, Cookies, Hashes, Tokens	1	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **firma y cifra bidireccionalmente las cookies**, aunque se intercepten no le sirven al atacante. El modelo firma y cifra bidireccional los hashes, sin embargo la manipulación directa de la memoria **podría comprometer los Hashes** del sistema, haciendo vulnerable el modelo. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado.
Overflow	Usuarios, Contraseñas, Cookies, Hashes, Tokens	1	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **firma y cifra bidireccionalmente las cookies**, aunque se intercepten no le sirven al atacante. El modelo firma y cifra bidireccional los hashes, sin embargo la manipulación directa de la memoria **podría comprometer los Hashes** del sistema, haciendo vulnerable el modelo. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado.
Pass-the-hash attack (PtH)	Hashes	S/D	No se cuenta con información para validar la vulnerabilidad del modelo frente a este tipo de ataques.
Phishing Real-time	Usuarios, Contraseñas, Tokens	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado.
Phishing Traditional	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
Physical Keylogger	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.

Shoulder surfing	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
Smishing	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
Social engineering	Usuarios, Contraseñas, Tokens	1	A pesar de los diferentes mecanismos de seguridad que incorpora el modelo, se asume que esta técnica podría llegar a evolucionar hasta lograr vulnerar al usuario.
Sql Injection	Usuarios, Contraseñas, Hashes, Tokens	S/D	No se cuenta con información para validar la vulnerabilidad del modelo frente a este tipo de ataques.
Vishing	Usuarios, Contraseñas	0	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada.
XSS	Usuarios, Contraseñas, Hashes, Tokens	S/D	El modelo **NO utiliza usuarios ni contraseñas,** autentica usando mensajería basada en llaves pública/privada. No se cuenta con información para validar la vulnerabilidad a nivel de **los hashes** del sistema ante esta técnica de ataque. El modelo **NO utiliza Tokens**, pues no es un modelo federado, se autentica en cada sistema accesado.
NIVEL DE VULNERABILIDAD		**4**	

Tabla 13 – Evaluación del nuevo modelo de IdM vs. las técnicas de ataque.

3.4 Evaluación de los sistemas y el modelo IdM vs. las técnicas de ataque

Al investigar y documentar los diferentes sistemas IdM utilizados por los 3 bancos y el modelo propuesto de IdM “Auto soberano con garante”, se identificó con base en el tipo de modelo de IdM y a las características de seguridad propias de cada sistema, el nivel de vulnerabilidad frente a las diferentes técnicas de ataques para el robo de identidad de cada uno de ellos. La tabla 14 nos muestra los resultados de la evaluación, teniendo en consideración estas convenciones: “0” significa que NO es vulnerable a la técnica; “1” significa que SI es vulnerable a la técnica y ”S/D” significa Sin datos para verificar si es o no vulnerable a la técnica. Este sistema de convención permite cuantificar la evaluación asignado un valor numérico en la evaluación.

EVALUACIÓN DE SISTEMAS IdM Y EL MODELO PROPUESTO VS. TÉCNICAS DE ATAQUE				
TÉCNICA	**Sistema IdM BANCO I**	**Sistema IdM BANCO II**	**Sistema IdM BANCO III**	**Modelo de IdM Auto soberano con garante**
Brute force	1	0	1	0
Directory Traversal	S/D	S/D	S/D	0
DNS hijacking	1	1	1	0
Sniffing	0	0	0	0
Execution Code	1	1	1	1
Exposed passwords	1	1	1	0
Http Response Splitting	S/D	S/D	S/D	0
Leaked databases	1	1	1	0
LSASS - Directory attack	S/D	S/D	S/D	S/D
Malware Banking trojans Webfilters	1	1	1	0
Malware Keyloggers	1	1	1	0
Malware Stealers	1	1	1	0
Man-in-the-Middle	0	0	0	0
Memory Corruption	1	1	1	1
Overflow	1	1	1	1
Pass-the-hash attack (PtH)	S/D	S/D	S/D	S/D
Phishing Real-time	1	1	1	0
Phishing Traditional	1	1	1	0
Physical Keylogger	1	0	1	0
Shoulder surfing	1	1	1	0
Smishing	1	1	1	0
Social engineering	1	1	1	1
Sql Injection	S/D	S/D	S/D	S/D
Vishing	1	1	1	0
XSS	S/D	S/D	S/D	S/D
NIVEL DE VULNERABILIDAD	**17**	**15**	**17**	**4**

Tabla 14 – Evaluación de los sistemas y el modelo IdM vs. las técnicas de ataque.

Como se puede apreciar en la tabla 14, el modelo de IdM mejor calificado y con el menor nivel de vulnerabilidad fue el modelo *Auto soberano con garante* - con un puntaje de 4 sobre 25, permitiendo con base a esta evaluación establecer que el modelo teórico de IdM auto soberano con garante puede ofrecer un mayor nivel de seguridad y una reducción significativa ante el riesgo por suplantación de identidad en los sistemas e-banking de Colombia.

3.5 Comparación de los sistemas y modelo IdM vs. Características ideales

Adicionalmente, se comparó el nuevo modelo de IdM auto soberano con garante contra las características observadas en los modelos de IdM de los 3 principales bancos del país, como se aprecia en la tabla 15, a continuación.

COMPARACIÓN DE SISTEMAS IdM Y MODELO PROPUESTO VS. CARACTERÍSTICAS IDEALES				
CARACTERÍSTICAS (Ideales para un sistema IdM)	**Sistema IdM BANCO I**	**Sistema IdM BANCO II**	**Sistema IdM BANCO III**	**Modelo de IdM Auto soberano con garante**
Tipo de Modelo de IdM	AISLADO	AISLADO	AISLADO	AUTO SOBERANO CON GARANTE
El sistema IdM permite que el dueño de la identidad sea el usuario	NO	NO	NO	SI
El sistema IdM verifica la identidad real de la persona que crea la identidad	SI	SI	SI	SI
El sistema IdM revela información solo con el consentimiento del usuario.	NO	NO	NO	SI
El sistema IdM ofrece al usuario control de su información en todo momento.	NO	NO	NO	SI
El sistema IdM almacena la información mínima posible.	NO	NO	NO	SI
El sistema IdM distribuye el almacenamiento de las identidades	NO	NO	NO	SI
El sistema IdM permite al usuario eliminar o renovar la identidad	NO	NO	NO	SI
El sistema IdM conserva evidencias y trazabilidad de acciones.	SI	SI	SI	SI
El sistema IdM generar confianza previniendo engaños al usuario	PARCIALMENTE	PARCIALMENTE	PARCIALMENTE	SI
El sistema IdM ofrece protocolos y tecnologías abiertas sobre su funcionamiento.	PARCIALMENTE	PARCIALMENTE	PARCIALMENTE	SI
El sistema IdM es compatible, amigable e intuitivo para los humanos	SI	SI	SI	SI
El sistema IdM protege las credenciales enviadas sobre una red de datos	SI	SI	SI	SI
El sistema verifica la fuente de la que está recibiendo credenciales	NO	NO	NO	SI
El sistema utiliza un modelo matemático público de comparación de credenciales	NO	NO	NO	SI
El sistema IdM protege su mensajería, evitando que pueda ser suplantada o alterada	SI	SI	SI	SI

Tabla 15 – Comparación de los sistemas y el modelo IdM vs. Características ideales.

Como se parecía en la tabla 15, el sistema propuesto de IdM auto soberano con garante, cumple con las 16 características idóneas que debe cumplir una solución de IdM, pues combina lo mejor de los modelos actuales de IdM tradicionales con las ventajas y fortalezas de blockchain, así como la descentralización del modelo mismo.

4. Conclusiones y recomendaciones

4.1 Conclusiones

- La administración de identidades es un reto en constante evolución, pues a medida que se desarrollan nuevos modelos y mecanismos de protección, los delincuentes evolucionan sus técnicas de ataque; en el desarrollo del presente trabajo, partiendo del estudio de las técnicas de ataque y explorando las ventajas de seguridad inherentes en blockchain, se logró proponer un nuevo modelo de administración de identidades basado en blockchain, que al ser comparado teóricamente con los modelos de IdM tradicionales, demostró una mayor capacidad de protección frente al riesgo por suplantación de identidad.

- La caracterización de las técnicas de ataque fue fundamental a la hora de establecer el nuevo modelo de IdM sobre blockchain; dicha caracterización, permitió entender las diferentes técnicas que utilizan los atacantes y los puntos vulnerables de los modelos de IdM tradicionales, evitando repetir estas debilidades en el modelo de IdM auto soberano con garante.

- Las diferentes soluciones de administración de identidades tradicional estudiadas en la presente investigación aportaron elementos clave a la hora de formular el nuevo modelo, permitiendo retar el paradigma de modelos de IdM centralizados y propietarios en cada entidad, para poder formular un nuevo modelo seguro, descentralizado, colaborativo, de bajo costo, alta disponibilidad y con menor exposición ante los riesgos de suplantación de identidad.

- Los buenos resultados observados en la comparación del modelo de IdM propuesto sobre las soluciones de IdM que utilizan actualmente los tres bancos analizados y la evaluación de las técnicas de ataque contra el modelo propuesto, permitieron responder a la hipótesis inicial formulada en este trabajo con un rotundo “si”, efectivamente el modelo teórico de IdM auto soberano con garante ofrece un mayor nivel de seguridad y una reducción significativa ante el riesgo por suplantación de identidad en los sistemas e-banking de Colombia.

4.2 Recomendaciones

Considerando los resultados positivos de la evaluación del modelo teórico, se plantea para futuros trabajos, el llevar el modelo propuesto del marco teórico al desarrollo técnico de una solución que opere contra la red de blockchain. Esto podría requerir el trabajo conjunto de un equipo de investigación y desarrollo mixto (Sovrin, universidad, empresa y gobierno) que permita avanzar en la construcción de un prototipo funcional para ser probado.

Bibliografía

[1] World Economic Forum, «WEF - Centre for Cybersecurity,» World Economic Forum, 5 sep, 2018. [En línea]. Available: https://www.youtube.com/watch?v=3JY4BZfV_LA. [Último acceso: 12 abr, 2019].

[2] Statista, «Número de usuarios de Internet en el mundo entre 2005 hasta 2019,» 2 nov, 2020. [En línea]. Available: https://es.statista.com/estadisticas/541434/numero-mundial-de-usuarios-de-internet/. [Último acceso: 20 mar, 2020].

[3] ONU, «Total population in millions 2020,» ONU, 2020. [En línea]. Available: https://www.unfpa.org/es/data/world-population-dashboard. [Último acceso: 7 abr, 2020].

[4] MinTIC, «Total de suscriptores de Internet en Colombia 2020,» MinTIC, 2020. [En línea]. Available: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-47275.html. [Último acceso: 14 abr, 2020].

[5] DANE, «CENSO NACIONAL DE COLOMBIA 2018 - Cuantos somos,» DANE, 2018. [En línea]. Available: https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivenda-2018/cuantos-somos. [Último acceso: 7 abr, 2019].

[6] Superfinanciera, «Informe de operaciones - segundo semestre 2019,» 26 feb, 2020. [En línea]. Available: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1043785/informetransacciones1219.docx. [Último acceso: 4 mar, 2020].

[7] IGI Global, «Encyclopedia of E-Commerce Development, Implementation, and Management,» IGI Global, 2016. [En línea]. Available: https://www.igi-global.com/dictionary/intermediaries-in-e-commerce/53303. [Último acceso: 25 feb, 2020].

[8] El Economista, «Diccionario de economía - banca electrónica,» El Economista, 2020. [En línea]. Available: https://www.eleconomista.es/diccionario-de-economia/banca-electronica. [Último acceso: 20 mar, 2020].

[9] Cambirdge Dictionary, «Cambirdge Dictionary - e-banking,» Cambridge University, [En línea]. Available: https://dictionary.cambridge.org/es/diccionario/ingles/e-banking. [Último acceso: 8 feb, 2020].

[10] Superfinanciera, «Circular Externa 050 del 2016 - F0000-141 formato 444,» Superfinanciera, 7 dic, 2016. [En línea]. Available: https://www.superfinanciera.gov.co/publicacion/10085860. [Último acceso: 24 nov, 2019].

[11] World Economic Forum, «WFE - Centre for cybersecurity,» 5 sep, 2018. [En línea]. Available: https://www.weforum.org/videos/world-economic-forum-centre-for-cybersecurity. [Último acceso: 7 abr 2019].

[12] World Economic Forum, «The global risks report 2020,» World Economic Forum, 13 feb, 2020. [En línea]. Available: https://www.weforum.org/reports/the-global-risks-report-2020. [Último acceso: 25 ene, 2020].

[13] IC3-FBI, «2019 Internet Crime Report,» FBI - Internet Crime Complaint Center, 10 feb, 2020. [En línea]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf. [Último acceso: 27 mar, 2020].

[14] Congreso de Colombia, «LEY 1273 DE 2009,» 5 enero 2009. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. [Último acceso: 8 sep, 2020].

[15] Policia Nacional, «Informe: Balance Cibercrimen en Colombia 2017,» Policia Nacional, 21 dic, 2017. [En línea]. Available: https://www.ccce.org.co/sites/default/files/biblioteca/policia-nacional-ciberseguridad.pdf. [Último acceso: 20 may, 2019].

[16] Policia Nacional, «Tendencias Cibercrimen Colombia 2019 - 2020,» Policia Nacional, 29 oct, 2019. [En línea]. Available: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf. [Último acceso: 14 feb, 2020].

[17] Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L. y & Margolis, D., «Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials,» de *ACM SIGSAC Conference on Computer and Communications Security*, Dallas, Texas, USA, 2017.

[18] Verizon, «2019 Data breach investigations report,» Verizon, 2 may, 2019. [En línea]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. [Último acceso: 28 nov, 2019].

[19] Symantec, «Symantec Internet Security Threat Report 2019,» Symantec, 19 feb, 2019. [En línea]. Available: https://www-

west.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf. [Último acceso: 25 11 2019].

[20] Blueliv, «The Credential Theft Ecosystem,» Blueliv, 23 oct, 2018. [En línea]. Available: https://www.blueliv.com/the-credential-theft-ecosystem/. [Último acceso: 31 10 2019].

[21] INCIBE, «Guía Nacional de Notificación y Gestión de Ciberincidentes,» INCIBE, 21 feb, 2020. [En línea]. Available: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf. [Último acceso: 24 mar, 2020].

[22] J. M. Esparza, «Understanding the credential theft lifecycle,» *Computer Fraud & Security,* vol. 2019, nº 2, pp. 6-9, feb, 2019.

[23] Microsoft, «Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 2,» Microsoft, 7 jul, 2014. [En línea]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=36036. [Último acceso: 12 abr, 2019].

[24] MITRE, «CVE Details,» MITRE Corporation, mar, 2020. [En línea]. Available: https://www.cvedetails.com/vulnerabilities-by-types.php. [Último acceso: 7 sep, 2020].

[25] H. L'Amrani, B. E. Berroukech, Y. E. B. El Idrissi y R. Ajhoun, «Identity management systems: Laws of identity for models evaluation,» IEEE, 24 oct, 2016. [En línea]. Available: https://ieeexplore.ieee.org/abstract/document/7804984/authors#authors. [Último acceso: 25 sep, 2019].

[26] K. Cameron, «The Laws of Identity,» Microsoft, 30 may, 2005. [En línea]. Available: https://msdn.microsoft.com/en-us/library/ms996456.aspx. [Último acceso: 12 10 2018].

[27] Optaris, «Doble Factor de Autenticación: categorías, métodos y tareas,» Optaris, 2017. [En línea]. Available: https://www.optaris.com/doble-factor-de-autenticacion-categorias-metodos-y-tareas/. [Último acceso: 5 may 2020].

[28] H. Loamrani, B. E. Berroukechy, Y. El Bouzekri y R. Ajhoun, «Identity Management Systems: Laws of Identity for Models Evaluation,» de *2016 4th IEEE International Colloquium on Information Science and Technology*, Tangier, Morocco, 2016.

[29] Okta, «Access Management - Gartner Magic Quadrant,» Gartner Inc., 10 2019. [En línea]. Available: https://www.okta.com/resources/access-management-leader-gartner-magic-quadrant/. [Último acceso: 14 04 2020].

[30] Okta, «Okta Investor Relations,» Okta, 1 abr, 2020. [En línea]. Available: https://investor.okta.com/. [Último acceso: 10 may, 2020].

[31] Oka, «Okta for Your Customer and Partner IAM Architecture,» Oka Inc., 10 oct, 2015. [En línea]. Available: https://www.okta.com/resources/whitepaper/iam-architecture/. [Último acceso: 17 may, 2020].

[32] Microsoft, «Administrador de identidades de Microsoft - Consideraciones relativas a la topología,» Microsoft, 12 oct, 2017. [En línea]. Available: https://docs.microsoft.com/es-es/microsoft-identity-manager/topology-considerations. [Último acceso: 29 feb, 2020].

[33] Ping Identity, «Ping Identity - Our Company,» 2020. [En línea]. Available: https://www.pingidentity.com/en/company/our-company.html. [Último acceso: 1 may, 2020].

[34] Ping Identity, «The Ping Intelligent Identity Platform,» Ping Identity, 2020. [En línea]. Available: https://www.pingidentity.com/en/platform/platform-overview.html. [Último acceso: 20 may, 2020].

[35] M. Smolny, «IBM Cloud Identity and Access Management — Overview,» IBM, 25 sep, 2019. [En línea]. Available: https://medium.com/@martin.smolny/ibm-cloud-identity-and-access-management-overview-fdd741bcabf. [Último acceso: 8 feb, 2020].

[36] Oracle, «Oracle Identity Manager – Business Overview,» Oracle, mar, 2013. [En línea]. Available: https://www.oracle.com/technetwork/middleware/id-mgmt/overview/oim-11gr2-business-wp-1928893.pdf. [Último acceso: 15 abr, 2020].

[37] T. Aste, P. Tasca y T. Di Matteo, «Blockchain Technologies: The Foreseeable Impact on Society and Industry,» *Computer Magazine,* vol. 50, nº 9, p. pp. 18 – 28, ene, 2017.

[38] Blockchain Federal Argentina, «Protocolos de consenso,» Blockchain Federal Argentina, 2019. [En línea]. Available: https://bfa.ar/blockchain/protocolos-de-consenso. [Último acceso: 25 mar, 2020].

[39] M. Gianpietro Zago, «50 examples of how blockchains are taking over the world,» 1 sep, 2018. [En línea]. Available: https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b. [Último acceso: 7 ago, 2019].

[40] P. Dunphy y F. A. Petitcolas, «A First Look at Identity Management Schemes on the Blockchain,» *IEEE Security & Privacy,* vol. 16, nº 4, pp. 20 - 29, 6 ago, 2018.

[41] B. Scriber, «A Framework for Determining Blockchain Applicability,» *IEEE Software,* vol. 35, pp. 70-77, ago, 2018.

[42] Sovrin, «Inevitable Rise Of Self-Sovereign Identity,» Sovrin Org., 29 sep, 2016. [En línea]. Available: https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/. [Último acceso: 1 nov, 2019].

[43] C. Dr. Lundkvist, R. Heck, J. Torstensson y otros, «uPort_whitepaper_DRAFT20161020,» uPort, 20 oct, 2016. [En línea]. Available: https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf. [Último acceso: 21 may, 2019].

[44] Civic Technologies, «Civic - Whitepaper,» Civic Technologies Inc., 9 jun, 2020. [En línea]. Available: https://www.identity.com/wp-content/uploads/2019/09/Civic-Whitepaper.pdf. [Último acceso: 16 jun, 2020].

[45] uPort, «Linkedin - uPort,» uPort, [En línea]. Available: https://www.linkedin.com/company/uport/about/. [Último acceso: 25 may, 2020].

[46] J. Vuong, «What is a uPort identity?,» uPort, 13 feb, 2019. [En línea]. Available: https://support.uport.me/hc/en-us/articles/360022530611-What-is-a-uPort-identity-. [Último acceso: 5 may, 2020].

[47] GLEIF, «Sobre la GLEIF,» GLEIF, 2020. [En línea]. Available: https://www.gleif.org/es/about/this-is-gleif. [Último acceso: 21 may, 2020].

[48] M. Wood, «PwC Onfido join blockchain identity platform uPort,» Ledger Insights, mar, 2019. [En línea]. Available: https://www.ledgerinsights.com/pwc-onfido-blockchain-identity-platform-uport/. [Último acceso: 21 may, 2020].

[49] D. Reed, J. Law y D. Hardman, «The Technical Foundations of Sovrin,» Sovrin Org., 26 sep, 2016. [En línea]. Available: https://sovrin.org/wp-content/uploads/2018/03/The-Technical-Foundations-of-Sovrin.pdf. [Último acceso: 30 nov, 2019].

[50] Sovrin, «Sovrin Technical Architecture Diagrams,» Sovring Org., 27 oct, 2016. [En línea]. Available: https://forum.sovrin.org/t/technical-architecture-diagrams/62/3. [Último acceso: 1 jun, 2020].

[51] K. Raj, «Foundations of Blockchain,» Oreilly, 2020. [En línea]. Available: https://www.oreilly.com/library/view/foundations-of-blockchain/9781789139396/659cc8cc-1110-4165-8c2d-90c7bc9da94e.xhtml. [Último acceso: 25 feb, 2020].

[52] J. Kassem, S. Sayeed, H. Marco y y otros, «DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network,» *Applied Sciences,* vol. 9, nº 2953, pp. 9 -15, 24 jul, 2019.

[53] Ping Identity, «Linkedin - ShoCard,» ShoCard Inc., mar, 2020. [En línea]. Available: https://www.linkedin.com/company/shocard-inc-/. [Último acceso: 25 may, 2020].

[54] Identity Technologies, «www.civic.com,» Identity Technologies Inc., 2020. [En línea]. Available: https://www.civic.com/. [Último acceso: 21 abr, 2020].

[55] P. Shoemaker, «The Identity Ecosystem - Civic Wallet,» Identity Technologies Inc., 19 nov, 2019. [En línea]. Available: https://www.identity.com/the-identity-ecosystem-civic-wallet/. [Último acceso: 15 jun, 2020].

[56] Colombia Fintech, «Primer hackathon blockchain de Colombia busca soluciones en e-commerce,» Colombia Fintech, 20 oct, 2019. [En línea]. Available: https://www.colombiafintech.co/novedades/primer-hackathon-blockchain-de-colombia-busca-soluciones-en-e-commerce. [Último acceso: 24 nov, 2019].

[57] Revista Dinero, «Así va el negocio de blockchain en Colombia,» Revista Dinero, 30 ago, 2019. [En línea]. Available: https://www.dinero.com/tecnologia/articulo/como-va-el-blockchain-en-colombia/275736. [Último acceso: 19 mar, 2020].

[58] Qubit Labs, «Portal Boletosqubit,» Qubit Labs, 2020. [En línea]. Available: https://www.boletosqubit.co/. [Último acceso: 19 abr, 2020].

[59] P. Mojica, S. Cuéllar y C. Medina, «Boletin Tecnologico - Blockchain,» Superintendencia de Industria y Comercio, jun, 2018. [En línea]. Available: https://www.sic.gov.co/sites/default/files/files/Propiedad%20Industrial/Boletines_Tecnologicos/Boletin_Blockchain.pdf. [Último acceso: 30 oct, 2019].

[60] R. Ferro, Y. Bernal y J. Tapicha, «Mejoramiento de la seguridad de los servicios del Estado: verificación de identidad e integridad de documentos, a través de Blockchain,» MinTIC - Centro de innovación, dic, 2017. [En línea]. Available: https://centrodeinnovacion.mintic.gov.co/es/investigaciones/mejoramiento-de-la-seguridad-de-los-servicios-del-estado-verificacion-de-identidad-e. [Último acceso: 19 nov, 2019].

[61] A. Shamir, «Identity-based cryptosystems and signatures schemes,» Weizman Institute of Science, 1998. [En línea]. Available: https://web.archive.org/web/20140203015750/http://islab.iecs.fcu.edu.tw/GroupMeeting/PowerPoint/g20050422_1.pdf. [Último acceso: 25 ene, 2020].

[62] C. Cocks, «An Identity Based Encryption Scheme based on Quadratic Residues,» 2001. [En línea]. Available: https://www.ime.usp.br/~rt/cranalysis/IBECCocks.pdf. [Último acceso: 15 mar, 2020].

[63] G. Ateniese y B. d. Medeiros, «Identity-based Chameleon Hash and Applications,» *Lecture Notes in Computer Science,* vol. 2003, nº 167, ene, 2003.

[64] NIST, «Norma NIST SP.800-162,» NIST, 8 feb, 2019. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf. [Último acceso: 19 abr, 2020].

[65] Qualys, «Qualys SSL Server Test,» Qualys, 2020. [En línea]. Available: https://www.ssllabs.com/ssltest/index.html. [Último acceso: 4 jul, 2020].

[66] P. Itusers, «Davivienda Elige solución de Easy Solutions Detect Safe Browsing,» Itusers, 16 feb, 2017. [En línea]. Available: https://itusers.today/davivienda-elige-solucion-de-easy-solutions-detect-safe-browsing/. [Último acceso: 14 abr, 2020].

[67] BBVA, «Apertura de cuenta online en BBVA,» BBVA, 2020. [En línea]. Available: https://cuenta.bbva.com.co/?tms-tagging-cta=cuentas_cuentaweb_comienzaaqui#!/steps. [Último acceso: 24 may, 2020].

[68] Bancolombia, «Bancolombia portal web personas,» Bancolombia, 2020. [En línea]. Available: https://sucursalpersonas.transaccionesbancolombia.com/mua/. [Último acceso: 29 mar, 2020].

[69] BBVA, «Portal transaccional BBVA Colombia,» BBVA, 2020. [En línea]. Available: https://www.bbva.com.co/. [Último acceso: 2 jun, 2020].

[70] Davivienda, «Portal transaccional Personas - Davivienda,» Davivienda, 2020. [En línea]. Available: https://www.davivienda.com/wps/portal/personas/nuevo. [Último acceso: 25 ene, 2020].

[71] Bancolombia, «Demo Sucursal Virtual Personas Bancolombia,» Bancolombia, 2020. [En línea]. Available: https://contenido.grupobancolombia.com/home/micrositios/demoSVP/. [Último acceso: 21 may, 2020].

[72] Davivienda, «Davivienda preguntas frecuentes,» Davivienda, 2020. [En línea]. Available: http://davivienda.custhelp.com/app/answers/detail/a_id/2433/related/1. [Último acceso: 28 ene, 2020].

[73] Bancolombia, «Aprender de seguridad en Bancolombia,» Bancolombia, 2020. [En línea]. Available: https://www.grupobancolombia.com/personas/aprender-es-facil/como-usar-banco/seguridad/. [Último acceso: 22 may, 2020].

[74] Davivienda, «Seguridad Davivienda,» Davivienda, 2020. [En línea]. Available: https://seguridad.davivienda.com/. [Último acceso: 25 mar, 2020].

[75] BBVA, «Seguridad en BBVA Colombia,» BBVA, 2020. [En línea]. Available: https://www.bbva.com.co/personas/recomendaciones-de-seguridad.html. [Último acceso: 29 may, 2020].

[76] Bancolombia, «Preguntas Frecuentes Bancolombia,» Bancolombia, 2020. [En línea]. Available: https://www.grupobancolombia.com/wps/portal/preguntas-frecuentes. [Último acceso: 21 may, 2020].

[77] B. A. Scriber, «A Framework for Determining Blockchain Applicability,» *IEEE Software,* vol. 35, nº 4, pp. 70 - 77, 6 agosto 2018.

[78] Verizon, «Verizon - our company,» Verizon, 7 feb, 2020. [En línea]. Available: https://www.verizon.com/about/our-company. [Último acceso: 31 mar, 2020].

[79] C. Allen, «The Path to Self-Sovereign Identity,» 25 abr, 2016. [En línea]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. [Último acceso: 16 mar, 2019].

[80] Real Academia Española, «Diccionario RAE - caracterizar,» Real Academia Española, 2019. [En línea]. Available: https://dle.rae.es/caracterizar. [Último acceso: 26 sep, 2019].