EL DESARROLLO DE CREDENCIALES DIGITALES COMO ESTRATEGIA DE APLICACIÓN EN COLOMBIA: EL USO DE LOS DATOS BAJO LA PERSPECTIVA PANDÉMICA

PRESENTADO POR:

JAVIER ALFREDO MONTERO HERNANDEZ

2285041

MODULO:

PROYECTO DIRIGIDO I

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGERIERIA DE TELECOMUNICACIONES

ESPECIALIZACION EN GESTIÓN DE REDES DE DATOS

BOGOTA D.C.

FEBRERO, 2021

Tabla de Contenido

Índice de tablas

TEMA: El desarrollo de credenciales digitales como estrategia de aplicación en Colombia: El uso de los datos bajo la perspectiva pandémica

Introducción

A nivel global, han surgido múltiples iniciativas orientadas a solucionar problemas que el Coronavirus Covid-19 ha traído a la nueva normalidad de los individuos y que cada país ha tenido que percibir de manera singular.

Es así que el mundo ha visto avances importantes es áreas como la medicina, la tecnología, la movilidad y las relaciones interpersonales. De allí que hayan surgido iniciativas como las Credenciales Covid, credenciales de orden digital que albergan datos personales y que están orientados a la simplificación de los procesos y la reactivación de los países bajo líneas éticas de estándares de Identidad Auto Soberana ISS, es decir manejar los datos de forma personal y cuidar la privacidad de los mismos.

Bajo esta perspectiva, la presenta investigación se encuentra orientada a determinar si el desarrollo de credenciales digitales se contempla como una estrategia de aplicación en Colombia que solucionaría diversos problemas que ha traído la pandemia por COVID-19 bajo la perspectiva del cuidado de los datos con estándar ISS.

Es así, que se realiza un análisis teórico que demuestra la base para el desarrollo y empleo de credenciales digitales o alternativas similares orientadas al mismo fin; posteriormente se realiza una investigación acerca del uso de las credenciales digitales y sus utilidades en el contexto global para posteriormente con la información recolectada determinar si existe viabilidad en el desarrollo de credenciales digitales como estrategia de aplicación en Colombia.

1. Justificación

En los países Europeos, se ha producido una transición de la utilización de documentos físicos hacia los documentos digitales denominados credenciales digitales, como una estrategia para simplificar la comprobación de datos entre partes y colaborar con las medidas de distanciamiento establecidas por los gobiernos. Estas credenciales han servido de base para la comprobación de los casos de COVID en países Europeos e incluso han servido de punto de

partida para Uruguay, el país Latinoamericano que mejor se encuentra preparado para la pandemia puesto que sugieren un modelo tripartito en donde se tiene un usuario, un emisor y un verificador; de esta simple manera se han podido realizar avances importantes para el monitoreo de los casos COVID, para la futura aplicación de vacunas de forma masiva y para la reactivación segura de la economía de los países

Para el caso Nacional, Colombia no es un país que se encuentre muy preparado para el uso de diversos mecanismos basados en la gestión de datos, pero más allá de ser visto como una falencia, es la perfecta oportunidad para obtener un mecanismo seguro, que proteja la privacidad de datos de los individuos y que a la vez colabore en la reactivación del contexto económico y social del país, los cuales se han visto afectados por el virus y las limitaciones que éste trae.

A nivel mundial, se ha generado un proyecto denominado Iniciativa de Credenciales COVID-19 (CCI) el cual es descrito por el director general de la Asociación GSM, Granryd (2020) como:

> Una comunidad global de más de 300 personas de más de 100 organizaciones que buscamos compartir nuestra experiencia, aprendizaje y conocimientos, y ayudarnos mutuamente a lanzar con éxito proyectos de credenciales verificables COVID-19 en las comunidades locales.

El proyecto, que ha reunido la atención global, insta a la creación de credenciales verificables de carácter digital y su misión corresponde a "Apoyar proyectos que utilizan Credenciales Verificables (VC) que preservan la privacidad para mitigar la propagación de COVID-19 y fortalecer nuestras sociedades y economías" Covid Creds (2020)

Por lo anterior, el proyecto busca analizar si el desarrollo de credenciales digitales se contempla como estrategia de aplicación en Colombia para el manejo de datos personales sanitarios, realizando un análisis de los resultados que las mismas han dado en otros países y realizando los ajustes pertinentes que permitan aplicarse a la singularidad del país, obteniendo así no solo una oportunidad de negocio importante, sino un avance significativo dentro de la reactivación del país, el seguimiento del virus y la facilitación de los procesos basados en la ética de los datos y la seguridad sanitaria que el país requiere. Lo anterior se ve reflejado en beneficios para los individuos (éticos), para el desarrollo de las actividades (prácticos), para el Estado (Seguridad sanitaria) y para la economía nacional (reactivación económica y social).

2. Formulación del problema

El mundo se ha visto enfrentado a innumerables cambios debido a la pandemia por COVID-19 que se ha venido presentado y que determinó una nueva normalidad en la cual todo gira alrededor del virus. En pro del manejo del virus y de no caer en las recesiones económicas, cada país le ha apostado a diversos mecanismos en los cuales el principal objetivo es determinar los casos positivos de COVID, rehaciendo un cerco epidemiológico y controlando lo mayor posible los contagios sin dejar de lado las actividad económicas, culturales y sociales necesarias para mantener la economía de la nación.

Para el contexto Colombiano, la aplicación CoronaApp ha otorgado información vital a los ciudadanos acerca del virus, formas de prevención y la opción para informar si considera posible que sea un infectado o presenta síntomas. Todos esos datos que se recolectan son de carácter sanitario urgente y por lo anterior pueden ser recolectados sin autorización del titular para los diversos usos que el Estado disponga. Lo anterior deslumbra una atmósfera de incomodidad en los ciudadanos que consideran vulnerados sus derechos a la privacidad y la confidencialidad.

No obstante, a pesar de contar con una aplicación y diversos mecanismos de monitoreo, no existe un sistema que pueda garantizar el seguimiento activo de los individuos sanos, infectados y recuperados y que a la vez simplifique los procesos permitiendo que se pueda verificar que los individuos que desarrollan ciertas actividades estén habilitados para hacerlo, puesto que son múltiples los casos en que infectados han salido a realizar actividades ya que no tienen ningún control ni monitoreo.

Con base a las anteriores razones, se evidencia la necesidad de diseñar un sistema que permita no solo monitorear cierta información delicada de los individuos, sino que les otorgue a ellos la capacidad de administrarla y así salvaguardar su confidencialidad, resumida dentro de una identificación digital personal, también denominadas credenciales digitales.

Por lo anterior, surge la pregunta ¿El desarrollo de credencias digitales se contempla como una estrategia de aplicación en Colombia que solucionaría el problema de monitoreo de datos personales sanitarios y su confidencialidad?; lo anterior desde la perspectiva pandémica del manejo de los datos recolectados por el COVID-19.

3. Gestión

A continuación se presentará el objetivo general y los objetivos específicos que guiaran el proyecto.

3.1. Objetivos

3.1.1. Objetivo General

Determinar como el desarrollo de credenciales digitales se contempla como una estrategia de aplicación en Colombia y qué soluciones puede brindar a los problemas que ha traído la pandemia por COVID-19

3.1.2. Objetivos Específicos

- Delimitar los avances en el desarrollo de credenciales digitales y proyectos afines bajo la investigación de los referentes teóricos relacionados con la temática a nivel global.
- Precisar cuál ha sido el uso de las credenciales digitales en el contexto global y que utilidades se han obtenido de dicho proceso.
- Determinar si existe viabilidad en el desarrollo de credenciales digitales como estrategia de aplicación en Colombia.

4. Marco referencial

A continuación se presentará el marco referencial que fundamentará el proyecto y funcionará como punto de partida para el desarrollo del mismo.

4.1.Marco teórico

4.1.1. Antecedentes

Tabla 1. Rejilla bibliográfica de antecedentes

1	**Certificados de inmunidad: Si debemos tenerlos, debemos hacerlo bien** **Autores:** GREUNER, D. Artículo de la Universidad de Harvard. Iniciativa de Impacto de respuesta rápida COVID-19. Artículo de investigación (20 de Abril de 2020) **Disponible en**: https://ethics.harvard.edu/files/center-for-ethics/files/10immunity certificates.pdf.
	El artículo científico de la Universidad de Harvard presenta un documento bajo principios éticos de la importancia que tiene el correcto manejo de los datos para la realización de certificados de inmunidad orientados a reactivar los países económicamente y lograr una nueva normalidad coordinada y segura. El artículo hace un repaso acerca de la arquitectura necesaria para la privacidad y la implementación de la equidad y protección de las libertades civiles. Finaliza concluyendo los pasos que se deben tener en cuenta a futuro y la utilidad de los certificados de inmunidad sin dejar de lado que preservar la salud pública no tiene por qué afectar o comprometer los derechos personales. El documento concluye resaltando el hecho de que los certificados digitales de inmunidad son la nueva fuente de información que los funcionarios de salud pública y los gobiernos necesitan para avanzar y recuperarse dando así pinceladas de la idoneidad de los Credenciales Digitales como una alternativa de solución ante el rezago que están viviendo las naciones y en específico el país Colombiano a causa de la pandemia por COVID-19.
2	**Una suave introducción a las credenciales verificables** **Autor:** HARDMAN, Daniel Artículo en el blog de la empresa Evernym. Noticias de la empresa. (02 de Octubre de 2020)

	Disponible en: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/
	La iniciativa parte del análisis de conversión de las credenciales tangibles que se usan, llámense licencias de conducir, certificados de nacimientos, certificados electorales, pasaportes, entre otros, hacia la transición como archivos digitales. Dichos archivos digitales aunque no son nuevos, si presentan avances a diario puesto que se reinventan bajo estándares criptográficos que los hacen poco vulnerables a manipulaciones. El artículo detalla beneficios para cada parte de los países que implementen dicha iniciativa, indicando que los gobiernos tienen vía libre para un nuevo crecimiento económico, las empresas obtendrán mejoras en seguridad, responsabilidad y automatización y los consumidores con la apertura hacia el mundo digital y la fase social mediante los pasaportes digitales. Se concluye que las identidades digitales obtienen beneficios principales como la simplificación de procesos en los intercambios de datos, en donde entidades de salud o seguros pueden ahorrar costos en verificación de datos. De igual manera, otro beneficio se representa en uno de los propósitos principales el cual es el control que tiene el titular sobre su identidad y la posibilidad de compartirla con quien desee y en la cantidad de información requerida.
3	**Identidad soberana y control de usuarios para preservar la privacidad del rastreo de contactos** **Autores:** SONG, Wenting. NOHKBEH, Razieh. LIAU, David. CHIH, Kai. LAMISON, Michael. KHALIL, Manah y BARBER, Suzanne. Biblioteca de la Universidad de Texas. Artículo de investigación. (30 de Noviembre de 2020) **Disponible en**: https://identity.utexas.edu/sites/default/files/2020-12/Self%20Sovereign%20Identity%20and%20User%20Control%20for%20Privacy-Preserving%20Contact%20Tracing.pdf
	La Universidad de Texas gestiona un acercamiento a los estragos que la pandemia por COVID-19 ha generado en la vida cotidiana de las personas y sus repercusiones en las diversas esferas que compone a cada nación. Como primera medida, se optó por el rastreo de contactos cercanos a los casos COVID positivo que representaba un cerco epidemiológico vital para frenar la velocidad de contagio. La anterior medida, aunque eficaz, supone un problema de privacidad para los individuos puesto que existen datos e

	información que se consideran sensibles al hacer parte de la vida personal de cada uno de ellos. Como medida ante esta posible vulneración de datos, se sitúa la Identidad Auto Soberana ISS como una alternativa de solución que ofrece a los usuarios la posibilidad de administrar sus propios datos de manera segura y decidir la cantidad de información que desean compartir cuando se es solicitada. Nuevamente, se generan nuevos interrogantes a futuro orientados a la confiabilidad por parte del usuario y su puesta en marcha a orden regional y global.
4	**Credenciales digitales para proteger la privacidad de los ciudadanos** **Autor:** Revista Latinoamericana E-Health reporter. Tendencias. 05 de Junio de 2020. España. **Disponible en:** https://ehealthreporter.com/es/noticia/credenciales-digitales-para-proteger-la-privacidad-de-los-ciudadanos/#
	Cada país de forma independiente ha lanzado diversas App para brindar información acerca del coronavirus Covid-19 y para recolectar datos que permitan conocer el estado del país en términos del virus pero ¿Las personas realmente aceptan la vigilancia de sus datos y la pérdida de su privacidad? Bajo esta premisa, la revista de salud desarrolla un análisis acerca de los esfuerzos mundiales para la creación de proyectos como lo son la iniciativa CCI orientadas a mitigar la propagación del Covid-19 mientras que se busca preservar la privacidad de los individuos y activar las economías de cada país. El artículo demuestra la amplitud de usos de lo que denominan como Credenciales Verificables o “VC” entre los cuales señalan principalmente el registro de los resultados de prueba de anticuerpos por Covid-19. Lo anterior indica que un individuo con una VC de prueba de anticuerpos positiva puede participar activamente de la reactivación social y económica de un país, a la vez que puede realizar actividades sociales y demás con el simple hecho de presentar dicha credencial de carácter digital.
5	**60 fuertes grupos de identidad soberana se enfocan en pasaportes y credenciales de inmunidad COVID-19** **Autor:** MORRIS, Nicky. Artículo Ledger Insights. Tecnología. (08 de Abril de 2020)

	Recuperado de: https://ledger-insights.com/sovereign-identity-covid-19-immunity-passports-credentials/
	A nivel global muchas empresas se han unido a la Iniciativa de Credenciales Covid CCI que ha instado a la utilización de la identidad digital como una estrategia para mitigar la propagación del virus. Esta iniciativa se ha enfocado en desarrollar pasaportes de inmunidad que les permitan a los individuos acreditar ciertos aspectos de su salud y que mediante el uso de la identidad auto soberana SSI garantiza la privacidad de los datos en donde es el individuo quien elige con quien compartir dicha información. Esta iniciativa está basada en un modelo tripartito en el cual el acceso a los datos está disponible únicamente para el emisor que vendría siendo una entidad hospitalaria/médica y el titular es decir el individuo. Para los fines necesarios, la certificación será presentada ante el verificador sin necesidad de que el individuo tenga que otorgar sus datos personales. El artículo concluye bajo la mirada de la unión de organizaciones destinadas a desarrollar las credenciales de inmunidad como una estrategia para la reactivación eficaz de los países, además de servir de instrumento seguro para realizar seguimiento a los casos activos del virus sin vulnerar en ninguna instancia la privacidad de los individuos.
6	**COVID 19: la identidad digital puede sacarnos del encierro, pero la confianza del usuario es clave** **Autor:** GRANRYD, Mats Blog empresarial. Artículo asociación GSMA. 30 de Abril de 2020. **Disponible en:** https://www.gsma.com/identity/covid-19-digital-identity-can-lead-us-out-of-lockdown-but-user-confidence-is-key
	La GSMA es la asociación que representa los intereses de los operadores móviles de todo el mundo integrando a más de 400 empresas referentes al sistema móvil, la fabricación y la creación de software. Este proyecto nace de la idea del cofundador de Microsoft, Bill Gates quién pidió el uso de la identidad digital el cual funcionaria como una estrategia para superar la recesión a través de certificados digitales que indiquen algunos elementos asociados al Covid-19 como los individuos afectados, recuperados, aquellos vacunados, entre otros. El artículo concluye con dos premisas importantes, por su parte se ve el papel central de la industria móvil frente a la nueva normalidad mundial. Los operadores son claves para

	el desarrollo de herramientas que permitan la utilización de los certificados digitales y es aquí donde nace la segunda premisa, la necesidad de desarrollo de dichos certificados a nivel global y su aceptación general, bajo medidas éticas de manejo de datos y bajo estándares de seguridad que impidan el fraude.
7	**Self-Sovereign Identity en la era de la pandemia: Validated ID se suma al Covid Credentials Initiative** **Autor:** PUEYO, Xavier. Artículo en el blog de la empresa Validated ID. Noticias y eventos. (29 de Agosto de 2020) **Disponible en:** https://www.validatedid.com/es/covid-credentials-initiative/
	El virus y su periodo de incubación de alrededor de 14 día ha imposibilitado la contención de la infección en la mayoría de los países y ante esto, muchos se han visto obligados a decretar cuarentenas u otros sistemas de distanciamiento. Con estas acciones, los gobiernos han visto las economías de sus países caer descontroladamente, lo cual ha llevado a pensar en estrategias de desconfinamiento eficaces que activen la economía y la sociedad sin recaer en los contagios desbordados y el colapso de los sistemas de salud. Por lo anterior, Validated ID, el gigante tecnológico, se ha unido a la Iniciativa de Credenciales Covid ICC a fin de aportar en el desarrollo de tecnologías que protejan los datos personales y respetan la privacidad de los individuos. El artículo deslumbra una realidad poco tratada en la cual el uso de credenciales digitales podría marginar ciertos individuos con características genéticas menos favorables y beneficiar a aquellos con sistemas inmunológicos mejor preparados, entendido como un privilegio para aquellas personas que estuvieron expuestas al virus y respondieron de manera favorable o asintomática a la enfermedad. Lo anterior deja ver que las discusiones éticas son consolidaciones que se presentan una tras otra y que deben ser valoradas con detenimiento para abordar el bienestar de todos los individuos.
8	**La identificación digital debe estar diseñada para la privacidad y la equidad** **Autor:** HANCOCK, Alexis Artículo. Fundación Frontera Electrónica. EFF. (31 de Agosto de 2020) **Disponible en:** https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10

	El artículo parte de las deficiencias en el diseño de las identificaciones digitales que pueden derivar en la invasión a la privacidad y la inequidad social. No obstante no de dejan de lado los beneficios como los son la simplificación de los procesos y el acceso a servicios gubernamentales de forma más rápida, entre otros. Las credenciales verificables representan afirmaciones digitales en las que confían tres partes, el emisor, el verificador y el titular de la misma. Las credenciales verificables basan su utilidad en las pruebas de conocimiento cero que son valores criptográficos en los cuales solo se presenta la información que solicitan, sin acceder a otro tipo de datos evitando que los emisores y verificadores tengan acceso a más información que la necesaria. El acceso a información privada puede derivar en casos de desigualdad en donde se margine a cierto grupo de individuos y es eso a lo que las credenciales verificables le apuntan bajo la visión de la ISS, Identidad Auto Soberana, un mecanismo que permite al titular de la información poseer sus propios datos y decidir qué cantidad de ellos compartir con los verificadores, sin existir una base que albergue los mismos y sin riesgo a perder la información.
9	**El pasaporte de inmunidad para acreditar el estado de salud a través de credenciales verificables y la blockchain** **Autor:** CALLIS, Silvia. Artículo en el blog empresarial BTC Assessors. 29 de Abril de 2020 **Disponible en:** https://btcassessors.com/blog/el-pasaporte-de-inmunidad-para-acreditar-el-estado-de-salud-a-traves-de-credenciales-verificables-y-la-blockchain/
	A través de la pandemia, el mundo ha visto una evolución en su forma de pensar y actuar frente a las adversidades, bajo esta mirada, la tecnología ha sido parte fundamental para crear soluciones que permitan reactivar las economías y los contextos sociales de los diversos países. El pasaporte de inmunidad nace de una premisa básica, los test masivos y las pruebas de anticuerpos pueden acreditar el estado de salud de un individuo frente al coronavirus Covid-19 y a su vez determinar de manera directa quien puede desempeñar tareas sociales libremente y quien debe estar bajo confinamiento.

	Bajo la anterior premisa, la situación decanta una posible alternativa, el uso de pasaportes de inmunidad que bajo el sistema de ISS, Identidad Auto Soberana puedan brindar una solución para la reactivación económica y social de los países sin afectar la privacidad de los datos de los usuarios.
10	**Como combatir una crisis sanitaria como la del coronavirus con ayuda de los datos** **Autor:** ZAIMOVA, Rositsa Artículo acerca de los desequilibrios globales del Covid-19. Foro Económico Mundial WEFORUM. (03 de Abril de 2020) **Disponible en:** https://es.weforum.org/agenda/2020/04/como-combatir-una-crisis-sanitaria-como-la-del-coronavirus-con-ayuda-de-los-datos/
	Muchos responsables de la sanidad pública encargados de tomas decisiones o generar directrices en los países frente al coronavirus Covid-19, carecen de datos de calidad y más que una oportunidad representan un riesgo frente a sus propios contextos. Por lo anterior, países como Bélgica han orientado grupo de trabajo en la utilización de datos anonimizados de operadores de telecomunicaciones a fin de determinar tendencias de movilidad lo cual permite generar estimados en donde se puedan determinar regiones con casos de brotes y el impacto de medidas en el ámbito socioeconómico. El dilema gira en torno a la privacidad de los datos y el uso que los gobiernos les dan a los mismos bajo prácticas éticas y cumplimiento orientado a las legislaciones sobre privacidad de los datos tanto en momentos de crisis al igual que al superar la pandemia. Se rememora aquella frase del director general de la OMS, Adhanom Tedros al indicar que “no se puede apagar un fuego con los ojos vendados” orientándola al concepto del beneficio que puede traer tener la información adecuada en las personas idóneas.
11	**Acuerdo para expedición de Constancias Digitales, como medida que promueva la identificación de las y los ciudadanos en sus trámites administrativos, con motivo de la declaratoria de emergencia sanitaria por la pandemia del coronavirus, Covid-19.** **Autor:** Consejo General del Instituto Nacional Electoral. INE/CG93/2020. 25 de Mayo de 2020. México D.C. **Disponible en:** https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/113984/CGex202005-15-ap-4.pdf
	Con motivo de la declaratoria de emergencia sanitaria por la pandemia del coronavirus Covid-19, el Instituto Nacional Electoral generó un acuerdo para expedir constancias

	digitales para los ciudadanos con fines administrativos. El INE observó necesaria la expedición de una constancia digital, la cual contará con una solicitud, emisión y envío a través de medios tecnológicos y funcionará como una modalidad de atención a la ciudadanía en carácter no presencial. Aunque corresponde a una estrategia de credenciales digitales para fines administrativos y en miras a cumplir con la atención de la INE a los ciudadanos, funciona como punto de inicio en el camino de la utilización de constancias digitales bajo la vista pandémica del coronavirus Covid-19 y su diversa utilización a nivel global. El proyecto tuvo una duración inicial de 3 meses y sirvió como medio entre los ciudadanos y todos los tramites que el Instituto desarrollaba devolviéndole así unas características sociales que la ciudadanía había perdido e instaurando dentro de la nueva normalidad del país un componente tecnológico. Finalmente, la viabilidad de su uso en los diversos programas del gobierno frente a la evolución de la pandemia, llevó a que el plazo de utilidad fuese ampliado estando vigente en la actualidad y siendo reconocido como exitoso.
12	**COVID-19 en personas con esclerosis múltiple: una iniciativa global de intercambio de datos** **Autores:** PEETERS, Liesbet; PARCIAK, Tina y WALTON Clare Revista de esclerosis múltiple. SAGE Journals. Artículo de investigación. (14 de Julio de 2020) **Disponible en:** https://journals.sagepub.com/doi/full/10.1177/1352458520941485
	El proyecto nace de la necesidad de obtener los suficientes datos de alta calidad que permitieran evaluar la gravedad del Covid-19 en pacientes de Esclerosis Múltiple. Por lo tanto se acordó la creación de un conjunto de datos centrales sobre Covid-19 en una muestra intencionada en la cual las variables se basaron en la infección por Covid-19, gravedad por infección, tratamiento, información demográfica e historial de Esclerosis Múltiples Las conclusiones del proyecto radican en la participación de 23 socios recopilatorios de datos de diversos países entre los cuales se lograron importaciones de datos enfocados en la enfermedad sin arriesgar los datos personales de los involucrados. Por consiguiente, la práctica clínica obtuvo muchos avances al comprender el efecto del Covid-19 en la

	enfermedad. El proyecto, que contaba con una misión clínica específica, derivó en un proceso de recolección de datos de varios países Europeos sobre el coronavirus Covid-19 y dio pinceladas acerca de los beneficios de la radicación de datos en múltiples escenarios.

Fuente: Elaboración propia, 2021.

4.1.2. Terminología

- **Aviso de privacidad**: Documento físico, electrónico o en cualquier otro formato (como puede ser visual o sonoro) generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con lo que establece la Ley. (IFAI, 2011)
- **Código QR:** Código bidimensional cuadrado que permite almacenar datos cuya característica es que se encuentran codificados, en la actualidad los códigos QR son utilizados en su mayoría para enlazar hacia URL de diversos sitios Web. (Unitag, 2020)
- **Credencial Verificable:** Afirmación emitida que contiene un conjunto de afirmaciones sobre un individuo u organización. El valor único de los VC es que son digitalmente nativos y criptográficamente seguros, lo que los convierte en una excelente alternativa para preservar la privacidad de otros tipos de credenciales, si se usan de manera responsable.(Covid Creds, 2020)
- **Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Departamento de función pública de Colombia, 2020)
- **Identidad Auto Soberana:** La identidad Auto Soberana o ISS por sus siglas en inglés corresponde a un modelo de las identidades digitales, en que cual una personas u organización puede poseer el control de los datos correspondientes a su identidad y

obtener independencia con las partes intermedias de los procesos de verificación (Covid Creds, 2020)

- **Iniciativa de Credenciales Covid-19**: Comunidad global de más de 300 personas de más de 100 organizaciones que buscan implementar y / o ayudar a implementar proyectos de credenciales verificables que preservan la privacidad a fin de mitigar la propagación de COVID-19 y fortalecer nuestra sociedades y economías.(Covid Creds, 2020)
- **Libertad Civil**: En su estado básico, el derecho civil define la libertad civil como el derecho de ejercer y hacer todo aquello que no se encuentra prohibido por la ley, presentando al beneficiario el acceso a su quehacer dentro de la libertad. (Enciclopedia jurídica, 2021).

4.2. Marco Legal

A continuación se presentará la normatividad que rige en el país y que fundamenta el desarrollo del proyecto

4.2.1. Artículo 15 Constitución política de Colombia

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley (…). (Ministerio de Comercio, Industria y Turismo, 2020)

4.2.2. Ley estatutaria 1266 de 2008

Se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Secretaria del Senado, 2020)

4.2.3. Ley estatutaria 1581 de 2012

Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Defensoría de Colombia, 2020)

4.2.4. Decreto 1727 de 2009

Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información, bajo unos requisitos mínimos de información general y obligaciones contraídas. (Sistema Único de Información Normativa, 2009)

4.2.5. Decreto 2952 de 2010

Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008 en donde se fundamentan los requisitos especiales para las fuentes de información, el incumplimiento de las obligaciones por fuerza mayor, el reporte de información negativa y la permanencia de la información negativa. (Sistema Único de Información Normativa, 2010)

4.2.6. Decreto 1377 de 2013

Por el cual se reglamentan aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas. (Alcaldía de Bogotá, 2013)

4.2.7. Sentencia C-1011 de 2008

Proyecto de ley estatutaria de habeas data y manejo de información contenida en bases de datos personales en el cual se fundamentan los requisitos especial de sus trámites, los criterios jurisprudenciales para determinar la validez, los propósitos y la inclusión de modificaciones o adiciones bajo la forma de artículos nuevos sobre asuntos previamente debatidos. (Corte Constitucional, 2008)

5. Propuesta de solución

A continuación se presentará la propuesta de solución sugerida ante el problema de investigación determinado, desarrollado a partir de diversos procesos sobre los cuales se conceptualiza la propuesta.

5.1. Aspectos conceptuales

Propuesta

Desarrollo de credenciales digitales como estrategia de aplicación en Colombia

La propuesta de solución plantea la creación de credenciales digitales, las cuales representan documentos de orden digital en donde se compila diversos tipos de información personal que puede ser presentada ante diferentes entes de control bajo ciertos contextos.

La credencial digital se desarrolla bajo un almacenamiento PDF, es decir Formato de Documento Portable cuya información se encuentra cifrada mediante un código QR y es presentada frente al ente que lo solicite para validar cierto tipo de información. Su característica principal se encuentra fundamentada en la Identidad Auto Soberana, la cual indica la capacidad del propietario o titular de administrar su propia información y decidir la cantidad de la misma que desea mostrar o dar a conocer cuando se le solicita.

Para el desarrollo de las credenciales digitales se requiere de modelos de datos, infraestructura, modelos de uso, sistemas de recopilación de datos y aplicaciones. Para su aplicación basta con contar con un celular Smartphone para presentar la información (titular), la cual es emitida por un ente certificado y regulado (Emisor) y un lector de códigos QR para leer y confirmar dichos datos (Verificador).

A fin de contextualizar la propuesta, el concepto de credenciales digitales se puede diversificar dentro de 3 categorías principales. La primera denominada **Identidad Digital** la cual representa la transición entre la documentación personal física en papel a la posesión de información en medios digitales y seguros bajo estándares de verificación, seguridad y practicidad.

La segunda categoría denominada **Identidad Auto Soberana** representa la capacidad del titular de la información de administrar sus datos y elegir a voluntad propia la cantidad de datos que desea presentar ante el ente verificador.

Por último se encuentra la categoría denominada **Modelo tripartito de la verificación de datos** representa un ecosistema en donde emisor / proveedor, titular y verificador interactúan bajo un sistema de confianza para asegurar la seguridad de un proceso bajo la veracidad de los datos necesarios.

Después de analizar el uso de las credenciales digitales y sus utilidades en el contexto global, se discierne la viabilidad de su uso dentro del contexto Colombiano con la premisa a priori de que cualquier estrategia debe ser ajustada a las particularidades de la región, basadas en economía, sociedad y cultura.

Lo anterior se entiende en que cada país es diferente, no solo en la parte normativa, sino en todos los contextos y por lo tanto una estrategia aplicada en un país no puede simplemente replicarse en otro porque claramente no va a funcionar ya que tienen particularidades totalmente opuestas.

Por lo anterior, el desarrollo de credenciales digitales como estrategia de aplicación en Colombia debe verse fundamentado bajo 3 ejes fundamentales:

- El primero de los ejes fundamentales será denominado **el desarrollo**, comprende la realización de las credencias digitales bajo la unión de empresas nacionales al proyecto global Covid Creds o un holding de organizaciones nacionales que se unan para su desarrollo dentro del país. Es importante determinar que el desarrollo debe tener una orientación mixta, es decir público-privada ya que la intervención del Estado es crucial para su futura puesta en marcha y el avance privado es importante para defender los derechos de las demás organizaciones y suponer un avance en los esfuerzos para el desarrollo de las credenciales en mención.
- El segundo eje fundamental será denominado **la normatividad y protocolos de seguridad**, comprende todas aquellas leyes y normas BASADAS en la Identidad Auto Soberana ISS, es decir la aseveración de que cada individuo manejará su propia información y obtendrá confianza al entender que sus datos no podrán ser

utilizados sin su autorización y los protocolos de seguridad basadas en la función criptográfica propias de las credenciales digitales que mitigarán los posibles fraudes o alteraciones a los datos y la vulneración de los mismos por parte de hackers u organizaciones delictivas.

- El tercer eje fundamental será denominado **el medio**, comprende la tecnología o medios tecnológicos que se utilizarán para dar vida al proyecto y para replicar su uso. En otras palabras, el proyecto de desarrollo de credencias digitales está orientado para uso desde el celular y por medio de protocolos bastante fáciles que aseguren que cualquier persona pueda utilizarlos de forma segura.

Dentro de este último eje juega un papel importante el dilema de la utilización de los Smartphone. Según el estudio del Ministerio de las TIC (2019) "Existen alrededor de 84.5 terminales por cada 100 habitantes" lo cual indica que aún existe un vacío importante en materia de tecnología en los ciudadanos. A 2020 es común encontrar individuos con celulares del año 2010 o menos, en donde claramente no podría funcionar un sistema u aplicación que permita asociar los datos de una credencial digital y esto representa una barrera importante para el proyecto, puesto que el éxito de una estrategia de esta magnitud es que el 100% de la población tenga acceso a los mismos. No obstante, la solución se encuentra realmente al alcance de las manos con un sistema que ya se está utilizando; cuando a una persona mayor o campesina se le solicita un correo para suministrarle alguna información, muchas veces suelen referir que no poseen pero que suministran el de algún familiar. Del mismo modo, puede aplicar para las credenciales digitales bajo el sistema de interfaz subtitular que fue mencionado con anterioridad, en donde un individuo poseía los datos sobre otro, bajo un justificante idóneo; aplicado a las Credenciales Digitales, un subtitular puede representar un miembro del hogar que posea un Smartphone y éste albergar las credenciales digitales de aquellos que no lo posean bajo la interfaz de subtitular.

En este punto, se deben rememorar las razones por las cuales se empezaron a desarrollar las credenciales digitales en el contexto global y observar si resultan idóneas para las necesidades del país. De esta manera, las credenciales digitales nacen desde un punto de vista pandémico, una estrategia para mitigar la proliferación del Coronavirus Covid-19 y para sistematizar las futuras vacunas que serán suministradas a la población; si nos detenemos en este punto, basta con

remitirnos a los boletines diarios del Ministerio de Salud para observar que aunque la curva de contagios por Covid-19 se ha aplanado un poco, las estimación son al aumento de casos dada la falta de cuidado de los ciudadanos y las múltiples protestas que se han venido presentando en el territorio nacional que son sinónimo de aglomeraciones.

Otra de las razones para la cual se desarrollaron las credenciales digitales es para evitar la proximidad entre partes cuando es necesario solicitar algún dato importante y a la vez tener la seguridad que los datos suministrados no serán motivo de vulneración de la privacidad. Bajo esta perspectiva nos encontramos a Colombia como un país en donde los trámites engorrosos son el diario vivir de las personas, en donde todo está dado por solicitar información constantemente de manera física puesto que los canales virtuales no son muy utilizados y la presencialidad es el factor común; de igual manera, encontramos los innumerables casos en donde los datos de los individuos son utilizados para diferentes fines que no son los dispuestos principalmente, bases de datos destinadas a fines políticos, falsedad en documentos para actos delictivos y llamadas extorsionantes bajo bases de datos de personas que suministraron información para actividades comunes son ejemplos de la vulneración de los datos de las personas. Si partimos de esta premisa, se evidencia la viabilidad de desarrollar las credenciales digitales en Colombia bajo diversos beneficios que se pueden obtener, en primer lugar se puede obtener beneficios en eficiencia puesto que las entidad que solicitan información pueden obtenerla de forma virtual y conservarla de manera ordenada para sus procesos propios. De igual manera bajo el principio de virtualidad, se simplificarían los procesos y más bajo la visión pandémica puesto que las personas no tendrían que acercarse a ninguna entidad sino que mediante una presentación verificable otorgarían la información que se les solicita y tendrían la oportunidad de otorgar únicamente los datos que desean sin sentirse vulnerados en su privacidad.

Por último se encuentra la reactivación económica; en Colombia al igual que en muchos países se dio paso de las pruebas para detectar Covid-19 hacia las pruebas para determinar los anticuerpos resultantes luego de superar la enfermedad ya que los anticuerpos determinan que un individuo no puede volver a infectarse con la misma cepa del virus y esto lo hace inmune y activo para la sociedad. Si tenemos ese precedente, porque no imaginar una reactivación económica y social en donde las empresas cuenten con la seguridad de que sus empleados presente credenciales verificables de que poseen anticuerpos contra la enfermedad o que son

casos negativos frente al Covid-19; porque no imaginar una reactivación social en donde las autoridades puedan tener un control de que las personas que realizan cierto tipo de actividades están habilitadas para realizarlo sin poner en peligro la vida de otros o la reactivación segura del sector turismo en donde las personas tengan la seguridad que en el lugar que están o aquellos otros grupos con quien comparte sean seguros en términos de Covid-19.

Todo lo anterior es posible bajo el desarrollo y posterior utilización de credenciales digitales dentro del contexto Colombiano, bajo líneas éticas de utilización de datos con el estándar ISS y bajo la sensación de seguridad presenta y vigencia de utilización a largo plazo, lo cual deslumbran la viabilidad para el desarrollo de las mismas en Colombia. En función de lo anterior y bajo la perspectiva de la pandemia por COVID-19 que el mundo afronta, se plantea el desarrollo de credenciales digitales que sirva como soporte para generar una nueva normalidad que no solo será aplicada a los inconvenientes que el Virus ha traído a nivel global sino que será un elemento utilizado post-pandemia dada su practicidad y viabilidad de uso para facilitar las actividades y procesos cotidianos que los individuos realizan a diario.

5.2. Planeación Metodológica

Para contextualizar el proyecto de desarrollo de credenciales digitales en función de las fases que requieren su planeación, se establecieron las actividades y procesos mínimos necesarios que garanticen el conglomerado de tareas que aseguren la viabilidad del proyecto para todos los contextos en los que se ejecute y cada una de las partes que en los mismos intervengan. Por lo anterior, se analizarán las fases de preparación, desarrollo, aplicación, comprobación y reestructuración así:

5.2.1. Preparación

Dentro de la fase de preparación del proyecto se consideraron los procesos de delimitación de casos de uso y delimitación de características esperadas. Ambos serán explicados de manera individual así

5.2.1.1. Delimitación de casos de uso

Es importante que durante la preparación del proyecto se identifiquen los principales casos de uso con sus responsables. Para lo anterior es importante identificar cuáles son los

principales integrantes dentro de una constancia digital los cuales corresponden a: Emisor, verificador, asunto y titular.

Con los principales integrantes identificados, se pueden establecer los principales entornos de uso que delimitaran los casos en los cuales serán utilizados. En este punto, es importante aclarar que los usos de las credenciales digitales son tantos como fines necesarios; no obstante existen ciertos conglomerados que son importante acatar en función de aquellas deficiencias o problemas que la pandemia por COVID-19 ha traído a la vida cotidiana de los países y sus ciudadanos.

El primero de estos conglomerados constituye la identidad neta del individuo y a su vez todos los componentes legales que su identidad requiere a nivel global para ser reconocido. Es este tipo de información la más utilizada para todo proceso. Con la información legal reconocida, el segundo conglomerado corresponde a la salud, un contexto bastante álgido en los últimos tiempos y que reunió la mayor atención dado que demostró la poca preparación que muchos países tenían en este tema y a su vez la capacidad de adaptarse rápidamente ante una adversidad. Con la llegada de vacunas a nivel global y el comienzo de la vacunación masiva, la idea de implementar un sistema de credenciales digitales para acreditar que alguien ha sido vacunado es una oportunidad para avanzar rápidamente en los procesos de reactivación social y económica. El tercer gran conglomerado corresponde a la educación, este contexto ha sufrido una gran adaptabilidad pero a su mismo tiempo ha abierto grandes brechas de desigualdad por la falta de capacidad para afrontar la virtualidad y la alternancia de parte de muchos hogares y muchos centros educativos. El cuarto conglomerado corresponde a las finanzas, este contexto es muy importante si se espera lograr una reactivación económica activa y prolongada en el tiempo; dentro de este conglomerado se pueden encontrar ventajas dentro de los servicios bancarios y los seguros y corresponden a ventajas específicas de practicidad, seguridad en las transacciones y digitalización.

5.2.1.2. Delimitación de características esperadas

A fin de contextualizar el proyecto, es importante delimitar cuáles serán las características que se esperará cumplan las credenciales digitales para así reglamentar en cierto modo su uso y dar una hoja de ruta de calidad que permita buscar la excelencia con el producto. La primera de estas características es la privacidad y seguridad al entender que las credenciales

digitales buscaran en todo momento respetar la privacidad y asegurar que los datos o declaraciones hechas por los emisores sean veraces.

La segunda de éstas es el ecosistema de confianza bilateral y avanzada que representa que entre las partes del modelo exista la confianza dada por la veracidad de ambas partes, la profesionalidad de los emisores y la seguridad de la información.

La tercera característica está dada a la independencia del proceso. Lo anterior está dado para que cuando un titular comparta la información, el emisor de la credencial no sepa la identidad del verificador; de igual manera un titular puede decidir en donde almacenar sus credenciales sin que el emisor sepa el lugar o cuando se accede a las mismas.

La cuarta característica está orientada a la revocación y actualización de las credenciales digitales; lo anterior está orientado a la capacidad de los emisores para revocar una credencial digital bajo ciertas circunstancias especiales y a su vez tener una opción de actualizar las credenciales ya sea por vigencia o revocatoria. Lo anterior tiene usos específicos como lo son las licencias de conducir, el respaldo crediticio, entre otros.

5.2.2. Desarrollo

Dentro de la fase de desarrollo del proyecto se consideraron las actividades de terminología de contexto, diversificación de tipos de objetos de informes y presentaciones verificables. Cada una de las anteriores será explicada individualmente así:

5.2.2.1. Terminología de contexto

La terminología de contexto es una alegoría a la necesidad de “hablar el mismo idioma” entre sistemas que se encuentren intercambiando datos. Dada la visión multisectorial a la cual se encuentra enfocada el uso de las credenciales digitales, es importante generar el concepto de “contexto” como un elemento que sintetice o acorte cierto tipo de información para obtener procesos más eficientes.

Puesto así, el contexto será visto como un “alias” que referencie ciertos tipos de información y ciertos entornos en los cuales será usado. Un ejemplo de lo anterior es entender el contexto de un certificado académico con el alias “@CertificadoUniSantoTomas” y englobar

todos los certificados de ese tipo bajo ese alías para agilizar el intercambio de información entre las diversas partes que lo necesiten.

5.2.2.2. Diversificación de tipos de objetos

Los tipos de objetos hacen parte de un conglomerado de datos verificables que permiten determinar la veracidad de una credencial digital y su pertinencia a la hora de justificar un proceso. Dentro de los tipos de objetos mencionados se encuentran:

El objeto de la credencial digital que representará el tema central de la misma; los objetos específicos que determinaran los subtemas o subgrupos acordes al tema central; el objeto de la presentación verificable la cual representa un conglomerado de credenciales digitales de un mismo usuario y que determinan múltiples partes de una misma personalidad; el estatus de la credencial que determinará su condición actual; los términos de uso y los objetos de prueba que representan la verificación y veracidad del documento.

Para garantizar que el intercambio de datos se trabaje de forma activa y se eviten los vacíos de in formación es importante que todas las credenciales digitales cuenten como mínimo con esos tipos de objetos y que su no implementación derive en la “no verificabilidad” de una credencial; en otras palabras, no contar con dicha información anulan su legitimidad. Sobra mencionar que todo tipo de información adicional será válido desde que se encuentre enmarcado en estándares de privacidad, accesibilidad y seguridad de la información

5.2.2.3. Presentaciones verificables

El concepto de presentaciones verificables hace parte de una visión de un contexto futuro en donde un individuo podrá manejar diversos tipos de credenciales digitales dentro de un mismo dispositivo. Esta variedad de información de un mismo titular es denominada presentación verificable y representa un conglomerado de datos que en la mayoría de casos refleja la realidad de un mismo titular. Lo anterior se aclara en función de que lo más importante dentro de la utilización de credenciales digitales es asegurar la privacidad de la información de los individuos que al ser personal muchas veces puede ser considerada sensible; por lo anterior se debe instar a que cada presentación verificable esté orientada salvaguardar la información y expresar solo aquellos tipos de datos que son necesarios, sin caer en aspectos de fuga de información o extralimitación de aporte de datos.

5.2.3. Aplicación

Dentro de la fase de aplicación del proyecto se consideraron los procesos de aspectos vitales y ciclo de vida de la credencial. Ambas serán ampliadas individualmente así:

5.2.3.1. Aspectos vitales

Dentro del proceso de aspectos vitales se busca dejar explícitas las partes que deben estar interactuando para que las credenciales digitales cumplan con su acometido según el uso que se les estén dando. Con respecto a lo anterior, las partes a interactuar son el **emisor** que cumple con la función de emitir una declaración acerca de un individuo; con la declaración realizada es importante especificar la **fecha de emisión** entendiendo que no se trata de la fecha en la que se crea la declaración sino de la fecha y hora en la que se vuelve valida dicha credencial (Se discierne que la fecha puede ser futura a la creación y sigue siendo igual de valida). Para continuar el proceso es importante que se especifique el **asunto** de la credencial dada la premisa de que un individuo puede contener credenciales digitales con información de diversos aspectos y para simplificar el proceso es importante mantener un orden a través del asunto de cada declaración.

Luego de contar con la información es importante añadir un modelo de **prueba** que promueva la seguridad y sirva como método de verificación; para este caso es importante añadir al menos una prueba criptográfica que asegure la veracidad de la información, la privacidad de los datos, la seguridad del sistema y mitigue los casos de alteración a la información. Del mismo modo es importante expresar la **fecha de vencimiento** de la credencial que represente la fecha y hora en la cual deja de ser válida la información allí presentada y emita una alerta al verificador (en el instante en que se compruebe la información) para que no se vaya a dar espacio a errores por omisión de verificación; dentro de este mismo aspecto influye el **estatus** o estado de la credencial pues es importante conocer si una credencial es revocada o suspendida ya que la mayoría de casos se presentarán cuando la credencial esté vigente y la omisión de estos datos puede dar paso a errores por omisión.

5.2.3.2. Ciclo de vida

Para que la aplicación del proyecto sea llevada a cabo con éxito es importante delimitar aspectos del ciclo de vida de las credenciales digitales, sus partes y roles.

En primer lugar del ciclo de vida de la credencial digital se encuentra el **emisor** quién siempre será el primero en intervenir pues es éste quien realiza una declaración acerca de un tipo de información y otorgándosela a un **titular;** este a su vez tiene la opción de almacenar dicho documento, borrarlo o transferirlo a otro titular a voluntad pues es de su propiedad. Para el caso de que deba presentar dicho información el titular podrá demostrar ante un **verificador** su credencial digital las veces que desee y este último tendrá la tarea de corroborar las afirmaciones que en el documento se encuentren. La **Credencial** podrá ser verificada en términos de estatus, fecha de emisión, fecha de vencimiento y legalidad. Por último se encuentra de nuevo el **emisor** con la voluntad de revocar la credencial digital emitida bajo conceptos que le justifiquen.

5.2.4. Comprobación

Dentro de la fase de comprobación del proyecto se considerarse los elementos de términos de uso y evidencia. Ambos elementos serán ampliados individualmente así:

5.2.4.1. Términos de uso

Para la fase de comprobación del proyecto es importe delimitar los términos de uso y actuar en favor de ellos para asegurar el funcionamiento de las credenciales digitales en base a elementos de legalidad y ética. Los términos de uso derivan en la respuesta a que cosas están permitidas hacer y cuales son prohibidas y reglamentan un uso ético de las credenciales digitales a través de cada uno de sus actores.

Por su parte, el emisor define unos términos de uso sobre los cuales se emite la credencial verificable y reglamenta los alcances que tendrá y su vigencia. De otro lado, el titular establece condiciones sobre las cuales puede ser utilizada su información y personalmente decide la cantidad de información que presentará ante el ente verificador. Bajo este tipo de propiedad denominado términos de uso, se le puede comunicar al ente verificador cuales son las acciones que tiene prohibidas realizar, aquellas que tiene permitidas hacer y aquellas que tiene por obligación verificar al momento de recibir la credencial digital. Al igual que todos los documentos tradicionales, aquel que no esté dispuesto a aceptar y cumplir con los términos de uso determinados se encontrara en desacato a la responsabilidad legal y será actor de violaciones a la ley.

5.2.4.2. Evidencia

Dentro de la fase de comprobación, es importante determinar que la confianza en la credencial digital esté sustentada en acciones de peso e información de respaldo; a lo anterior se le denomina evidencia. La evidencia pasa a ser toda esa información o procesos de verificación de datos que el emisor realiza a priori y le garantizan que aquella afirmación que emitirá está sustentada en términos éticos y de veracidad. Este proceso no solo beneficia al emisor sino que es una base de confianza para que los verificadores asuman los riesgos que implican aceptar la información detallada en una credencial digital. Dentro de este ítem se puede entrar en un dilema ético puesto que la premisa por la que se vela es la no necesidad de revelar información adicional para salvaguardar la privacidad del titular, no obstante, prima el bienestar colectivo sobre el personal y la necesidad de adquirir datos se considera un procesos justificante para actuar en términos de confianza entre los actores del ecosistema.

5.2.5. Reestructuración

Dentro de la fase de reestructuración del proyecto se enfocan las acciones hacia la revalidación y los patrones de uso, que determinan acciones que se pueden cambiar en función del uso de las credenciales digitales. Cada una de estas será explicada individualmente así

5.2.5.1. Revalidación

El proceso de revalidación se encuentra orientado a solventar la actualización de las credenciales digitales cuando acaban su proceso de validez. Como fue mencionado en el proceso de aspectos vitales de la fase de aplicación, las credenciales digitales cuentan con una fecha de vencimiento establecida y para algunos casos la continuidad de dicha validez es un tema obligatorio por lo anterior la opción de actualización de las credenciales se convierte en una necesidad.

Si se tiene en cuenta que uno de los propósitos principales de las credenciales digitales es promover la practicidad de las tareas en términos de eficiencia, intercomunicando entre partes sin la necesidad de un encuentra presencial y promoviendo la digitalización se deben establecer acciones orientadas a realizar actualizaciones de las credenciales digitales de manera automática (mientras las especificaciones de la información lo permitan) y manual (cuando conlleve actualización de datos pero de manera digital).

De igual manera es importante rellenar los vacíos de seguridad que la actualización automática puede presentar, obligando a que dicha opción se encuentre disponible únicamente en el dispositivo del titular y bajo un proceso bilateral con el emisor puesto que se puede prestar para que verificadores actualicen de manera privada las credenciales de los titulares sin contar con su consentimiento.

5.2.5.2. Patrones de uso

El uso generalizado de las credenciales digitales tiene múltiples beneficios a la hora de ayudar en la práctica cotidiana de los individuos; no obstante, es importante analizar los efectos adversos que se pueden presentar y plantear estrategias que lleven a mitigar dichas situaciones.

Es importante establecer que los efectos adversos están basados en supuestos y que su presencia o no, radica netamente de las variables que en la aplicación se presentan y las condiciones particulares que cada contexto determina. Puesto así, se plantean que la mayoría de efectos adversos estarán dados por inferencia de uso; lo anterior se puede explicar con el ejemplo de uso de credenciales, si una credencial digital es presentada más de una vez a un verificador, con el tiempo el sistema o la simple recordación harán pensar que aquella persona que demuestra la credencial es el titular, pero como el medio en muchos casos es virtual, puede que quien presenta la credencial sea un agente externo.

La segunda eventualidad que puede tener mayor incidencia es aquella orientada a la fuga de información o el acceso de la misma de forma voluntaria e ilegal. Nuevamente lo anterior es explicado mediante el ejemplo de uso; si una persona utiliza una credencial digital ante diversos verificadores, estos últimos pueden colaborar de manera ilegal para compartir la información y así generar un nuevo registro con la información compartida de ambos verificadores y datos adicionales que no fueron compartidos en uno de los diversos verificadores.

Es importante recalcar que dichas eventualidad solo son medibles en la calidad que la aplicación del proyecto se ejecute pero pueden ser mitigadas u orientadas a mitigar bajo acciones previas enfocadas a la consecución de la privacidad y la no anonimización. La primera de estas acciones será aquella orientada al uso de un identificador único que garantice la titularidad de la credencial y su uso, lo anterior permitirá que no se asuma que quien presente la credencial sea el titular y ayude a evitar los problemas de seguridad por uso continuo. La segunda acción estará orientada a la búsqueda de un servicio global para actualización y revocación de credenciales

digitales, lo anterior es útil ante vacíos en los sistemas de diversos entes, puesto que puede que una credencial revocada sea utilizada en entidades que aún no cuentan con la información que acredite que dicha certificación fue revocada y se presenten problemas legales.

5.3. Desarrollo tecnológico

Para contextualizar el proyecto de desarrollo de credenciales digitales en función de las fases concernientes a los aspectos tecnológicos y técnicos, se establecieron las actividades y procesos mínimos necesarios que garanticen el conglomerado de tareas que aseguren la viabilidad del proyecto para todos los contextos en los que se ejecute y cada una de las partes que en los mismos intervengan. Por lo anterior, se dividieron dichos procesos en 3 grandes grupos, el grupo de privacidad, seguridad y accesibilidad.

5.3.1. Privacidad

En función de promover la privacidad de los usuarios entorno a la utilización de las credenciales digitales se establecieron 3 procesos principales de orden tecnológico y técnico fundamentados en las pruebas de conocimiento cero, espectros de privacidad y huellas digitales. Cada uno de los mencionados será ampliado de forma individual así:

5.3.1.1. Prueba de conocimiento cero

La prueba de conocimiento cero es un método criptográfico orientado a demostrar que se conoce una información sin tener que demostrar todos los datos con los que se cuenta. En contexto, un verificador puede solicitar un dato para acreditar un proceso y el emisor presentará dicho dato contenido en una credencial digital sin tener la necesidad de enseñar toda la demás información contenida en la mencionada credencial.

Lo anterior, le otorga al titular la posibilidad de proporcionar la información netamente solicitada sin caer en la fuga de datos por acción voluntaria. Lo anterior supone que los emisores evoquen esfuerzos para que las credenciales estén orientadas a mejorar cada vez más la privacidad de los titulares. En otras palabras, desde el inicio del modelo tripartito de verificación de datos el emisor evocará un proceso de privacidad que será mantenido a través de todo el ecosistema y así se garantizará que las credenciales digitales satisfagan el vacío de privacidad por el cual se ha luchado desde el comienzo del proyecto.

5.3.1.2. Espectro de privacidad

Después de que el ecosistema de las credenciales se encuentra orientada a preservar la privacidad es importante delimitar que alcance tiene ese espectro de privacidad para orientar los esfuerzos en función de los límites. Según las tendencias, se conoce que la mayoría de personas optan por mantener el anonimato en la mayoría de actividades que realizan cuando se les solicitan otros datos para continuar el proceso. Por ejemplo en muchos casos los requisitos de un proceso es contar con la legalidad de edad (18 años en el país); para estos casos el requisito de datos personales como el nombre e información adicional no es necesaria. Caso contrario existen elementos que requieren el nombre y número de identificación del titular sin que la edad sea un requisito necesario.

Lo anterior permite entender que existen diversas situaciones de privacidad según el contexto en el cual se esté desenvolviendo la necesidad de información. Por lo anterior no se puede suponer que exista un nivel de anonimato mínimo o máximo a establecer sino por el contrario, velar por la privacidad de una persona es a la vez disponer de legitimidad para que cada uno determine hasta dónde quiere llevar la misma sin afectar las correctas relaciones entre los actores que intervienen en el proceso de las credencias digitales.

5.3.1.3. Huellas digitales

Dentro del apartado tecnológico es importante hacer un llamado a todos aquellos mecanismos externos que se utilizan para conseguir datos y rastrear información de las personas y que junto con las credenciales digitales pueden suponer un problema en la privacidad de los usuarios. Estas tecnologías denominadas de seguimiento son autónomas y es imposible evitar su uso puesto que hacen parte de un conglomerado de búsqueda de datos propio de los dispositivos. Por lo anterior lo idóneo es hacer un llamado al respeto de la privacidad de las personas, evitando el rastreo de todas las huellas digitales que se dejan en los dispositivos y para que la información de las credenciales digitales no sea manipulada u obtenida de manera externa.

5.3.2. Seguridad

En función de promover la seguridad de los usuarios de las credenciales digitales, se plantean 3 procesos principales de orden tecnológico y técnico denominados credenciales de 1

solo uso, protección integral y robo y suplantación. Cada uno de los mencionados será analizado individualmente así:

5.3.2.1. Credenciales de un solo uso

Aunque la practicidad del uso de las credenciales digitales es un proceso que fundamenta en mayor medida la viabilidad de su aplicación, se tiene como precepto que para favorecer la seguridad de los datos de los usuarios la mejor alternativa es optar por la medida de generar credenciales que solo sean usadas 1 vez.

Se entiende que el uso de credenciales digitales con identificadores de larga duración solventaría problemas de practicidad desde cierto punto de vista; no obstante, que el ecosistema esté enfocado en la privacidad y la mínima interacción con los datos requiere plantearse dichas propuestas en donde las credenciales de un solo uso sean usadas ante el ente verificador y este deseche los "residuos" de datos a fin que no quede información activa bajo la tenencia de ningún elemento exceptuando al titular.

5.3.2.3. Protección integral

Otro de los aspectos a revisar dentro de las credenciales digitales es aquel orientado a corroborar datos externos que residen en bases de datos ajenas a la credencial digital. Lo anterior entendido como la capacidad de las credenciales digitales de albergar URL que re direccionen a fuentes externas para corroborar datos o conocer otros tipos de información en diversos medios (llámense imágenes, contextos, entre otros).

Dado que estos tipos de datos residen en fuentes externas no se pueden controlar ni asegurar su confidencialidad a terceros, por lo tanto lo ideal es hacer un llamado a los usuarios a asegurarse que tipo de información reside en medios externos y si las URL cuentan con mecanismos avanzados de protección integral

5.3.2.4. Robo y suplantación

Como último elemento se debe considerar aquel contexto en el que el usuario pierde su dispositivo (en donde residen sus credenciales verificables) y queda afectada la seguridad de sus datos y su vida digital. Por lo anterior se deben plantear medidas generales a fin de mitigar el riesgo. En primer lugar y quizá la más básica está orientada a la protección tecnológica del dispositivo en sí y su acceso, en este caso la protección de desbloqueo del dispositivo juega un

papel primordial asegurando que mediantes contraseñas, patrones o elementos biométricos dificulte el acceso al contenido del dispositivo. En segundo lugar se debe instar para habilitar autenticación (llámense contraseñas o biométrica) a elección del usuario mediante las cuales se pueda acceder al portafolio de credenciales o las claves criptográficas propias de cada Credencial digital.

5.3.3. Accesibilidad

Como último grupo para el desarrollo del proyecto en términos de carácter tecnológico y técnico se encuentra la accesibilidad el cual cuenta con el proceso denominado “Datos primero” entendido así:

5.3.3.1. Datos primero

En términos de accesibilidad se discierne que las credenciales digitales contarán con múltiples beneficios dadas su naturaleza y diversificación para los contextos en los que sean requeridos en comparación con sus antecesores físicos. No obstante, es importante determinar las falencias de sus antecesores para no caer en los mismos errores, por tal razón se determinó que la calidad de los datos es un tema que debe ser primordial para obtener una accesibilidad deseada. Dentro de lo mencionado se sugiere un diseño intuitivo, sobrio y con un enfoque orientado a las necesidades de cada gran grupo de personas.

Con lo anterior se quiere dar a entender que se dejan atrás las certificaciones con problemas de lectura, en donde se deben hacer maniobras para leer el contenido deseado o que puede significar un problema para personas con déficit de visión para pasar a un modelo concreto, con un tamaño de letra adecuado, el logo o imagen de la dependencia que emite la certificación y los datos específicos a la vista a fin de satisfacer las necesidades de todos los actores del ecosistema de confianza de las credenciales digitales.

6. Conclusiones y proyecciones

Abordar el desarrollo de credenciales digitales como estrategia de aplicación en Colombia desde una perspectiva pandemia otorga múltiples beneficios a la visión del proyecto y permite prepararse de mejor manera al proceso investigativo al estar orientado netamente a aplicaciones que beneficien las deficiencias que la pandemia por COVID-19 ha traído a todas las naciones y en especial a Colombia.

El panorama global a futuro por la pandemia del Coronavirus Covid-19 es realmente incierto pero existe una premisa que es conocida por todos y que es necesario analizarla, aquellos países fuertes y desarrollados tendrán mejores herramientas para volver a iniciar de forma exitosa y sin tantas consecuencias y aquellos países en vías de desarrollo y con problemáticas nacionales tendrán la peor parte y las barreras más notorias.

La propuesta de credenciales digitales en primera instancia demostró su capacidad para ayudar a reactivar aquellos sectores que fueron fuertemente golpeados por la pandemia y las medidas de confinamiento orientadas a la preservación de la salud que fueron adoptadas mundialmente. Bajo el desarrollo de credenciales digitales se obtuvieron múltiples aspectos positivos en términos de reactivación económica y social del país (Las cuales son las principales que mueven el país) asegurando en todo el proceso la seguridad sanitaria de los múltiples actores que intervienen en muchas de las actividades cotidianas.

Teniendo lo anterior como referencia se puede obtener un bosquejo positivo de la viabilidad del desarrollo de credenciales digitales como estrategia de aplicación para el país. No obstante, entre más se avanza en el tema, más son las obligaciones con las que se deben cumplir para ofrecer una solución integral enmarcada en términos éticos de protección y seguridad.

Avanzar en el tema, dibujó un contexto en el cual la privacidad de los individuos y la seguridad de sus datos se volvió en un aspecto fundamental en el cual las credenciales digitales debían enfocarse para cumplir con un proceso importante sin alterar los derechos básicos de cada individuo. Puesto así nuevamente surgen más condicionantes entre más se avanza en el tema que aunque tienen solución de diversas medidas, deben plantearse para el contexto netamente Colombiano y sus características propias.

Lo anterior, genera un sentir de preocupación de la capacidad del país para hacer una transición prolongada en el tiempo hacia la digitalización y que en el proceso se asegure un modelo de confianza en su utilización y un sistema de privacidad y seguridad para los usuarios. Dicha preocupación se sustenta en los vacíos tecnológicos que se presentan en el país y el abandono tecnológico (y económico) en el que muchas ciudades se encuentran por parte del gobierno nacional, los condicionantes culturales que muchas veces ejercen mucha fuerza e impiden un avance en la mentalidad y actuar de las personas y las faltas éticas que se han vuelto un tema común y recurrente en donde la trasgresión de la libertad personas y su integridad se considera un evento natural en una sociedad con graves deficiencias éticas.

El desarrollo de credenciales digitales podría solventar muchos problemas que ha traído la pandemia por COVID-19 y muchos oros más que el atraso técnico y cultural ha dejado a su paso en el país. Colombia en estos momentos se encuentra en un proceso irrisorio de inicio tardío de vacunación lo cual comprueba que la pandemia y sus estragos permanecerán en el país por un tiempo largo; lo anterior funciona como condicionante si se quieren determinar las credenciales digitales como una opción para acreditar información acerca del virus. Si por el contrario se quiere hablar de las vacunas, el sentir general y casi que unificado es que el tema de vacunación se prestará (al igual que casi todo en el país) para temas de corrupción, malversación de fondos y favorecimiento a terceros; en este contexto el desarrollo de credenciales digitales servirá como un sistema que acreditará de manera real la aplicación y destino real de dichas vacunas. Por otro lado desde un contexto educativo, las credenciales digitales solventaran desde problemas teóricos como la solicitud de certificados estudiantes, diplomas, información educativa, notas, entre otros, hasta problemas prácticos como la vuelta a clases presenciales de forma totalmente segura.

Al analizar estos contextos se pueden ver aspectos positivos del desarrollo de credenciales digitales como estrategia de aplicación en el país sin embargo en el proceso investigativo se observó que la viabilidad de su uso no se encuentra condicionante a la pandemia y sus enfoques, sino que por el contrario el mayor provecho del proyecto se encuentra dentro del largo plazo en la diversificación de uso como una herramienta que cumplirá con el propósito principal de la tecnología: hacer la vida de los individuo mucho más fácil. Son las credenciales digitales la llave al mundo híper conectado que refleja beneficios en la vida de las personas, un mundo que cada vez es más latente y que al igual que se ha dicho en los últimos 10 años es un

mundo en el cual aquellos que no estén preparados para afrontarlos quedaran rezagados y serán excluidos por el propio sistema.

Llegado el punto de entender la viabilidad del desarrollo de las credenciales digitales, es importante prestar especial atención a aquellos aspectos que significaron las principales barreras en la implementación del proyecto. Por un lado, la capacidad tecnológica del país es un elemento que debe ser analizado cuidadosamente; en este aspecto entra a escena una hipótesis obtenida durante la investigación la cual se encontraba orientada a la utilización de las credenciales digitales en un país en el cual aún se encuentran muchas personas que no cuentan con la capacidad de adquirir Smartphones o aquellos de avanzada edad que no cuentan con el conocimiento técnico necesario para su utilización. Por otra parte el tema cultural y ético del país es un tema que debe mantenerse en consideración a fin de generar estrategias focalizadas en robustecer las características de privacidad y seguridad que defienden, en teoría, las credenciales digitales y bajo las cuales se generaron los diseños de ejecución del proyecto.

Colombia es un país con viabilidad para tener éxito en todos los desafíos que quiera enfrentar pero curiosamente las barreras para esto siempre se encuentran dentro del mismo entorno. Aunque parezca una frase cliché realmente la unión representa el éxito y para Colombia es una necesidad más que una opción. Es necesario unir gremios, estados y ciudadanía en pro de reactivar la economía y sociedad de manera segura para mitigar las consecuencias en la calidad de vida de los ciudadanos y en esta tarea el uso de la tecnología es clave para lograr las metas planteadas de forma eficaz.

El proyecto tiene todas las características para ser un caso de éxito con la coordinación adecuada y el apoyo de múltiples entornos para asegurar su funcionamiento y su alcance generalizado a toda la población meta, demostrando que muchas veces las adversidades son la puerta a los mejores proyectos.

Recomendaciones

Como recomendaciones finales se plantean dos aspectos principales, la primera recomendación orientada al lector a la conceptualización del tema y la búsqueda por la participación activa del mismo entendido como seres socialmente activos en donde la búsqueda del bien general sea primordial y se apropien del tema y el proyecto como si fuera personal. Lo anterior se hace en función de que todo proyecto puede ser alcanzado y abarcado en mayor medida desde que se cuente con el apoyo y unión de múltiples actores de la sociedad.

Por otra parte se hace un llamado a los investigadores, ya sea en esta línea o como sistema de detracción. Un tema adquiere valor cuando existe evidencia investigativa y científica que lo respalde y ese es uno de los propósitos principales de esta investigación, enriquecer la cantidad y calidad de material investigativo en torno al tema, así como el contexto científico que se oriente en todo momento a facilitar la vida de los individuos, primer objetivo de la tecnología.

Como resultado del proceso investigativo se hace especial énfasis en el llamado a los investigadores en realizar procesos investigativos orientados a conocer la capacidad financiera que un proyecto de tal magnitud refiere y las líneas de financiamiento que pueden ser alcanzadas para sintetizar el proyecto y traerlo a la realidad. De igual manera, es importante realizar procesos investigativos en términos de alcances, impactos en la sociedad, vacíos investigativos y medios para abarcar de manera real toda la población esperada en un esfuerzo por traer la digitalización a la vida de los Colombianos y alcanzar una nueva era enfocada en los beneficios para los individuos a través del desarrollo de credenciales digitales.

Referencias

Alcaldía de Bogotá. (2013). Decreto 1377 de 2013. Recuperado de: https://www.alcaldiabogota .gov.co/sisjur/normas/Norma1.jsp?i=53646#0. (09 de Septiembre de 2020)

Callis, S. (2020). El pasaporte de inmunidad para acreditar el estado de salud a través de credenciales verificables y la blockchain. Artículo empresarial. BTS Assessors. Recuperado de: https://btcassessors.com/blog/el-pasaporte-de-inmunidad-para-acreditar-el-estado-de-salud-a-traves-de-credenciales-verificables-y-la-blockchain/. (09 de Septiembre de 2020)

Corte Constitucional. (2008). Sentencia C-1011/08. Proyecto de ley estatutaria de habeas data y manejo de información contenida en bases de datos personales. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm. (09 de Septiembre de 2020)

Covid Creds. (2020). Covid-19 Credentials Initiative. ¿Qué es CCI? Recuperado de: https://www. covidcreds.com/#Blog. (08 de Septiembre de 2020)

Covid Creds. (2020). Covid-19 Credentials Initiative. Our Mission. Recuperado de: https://www. covidcreds.com/#Blog. (08 de Septiembre de 2020)

Defensoría de Colombia. (2020). Ley estatutaria 1581 de 2012. Recuperado de: https://www. defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf. (09 de Septiembre de 2020)

Departamento de función pública de Colombia. (2020). Gestor normativo Concepto 121121 de 2020. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma. php?i=127931#:~:text=Para%20los%20prop%C3%B3sitos%20de%20la,o%20filos%C3 %B3ficas%2C%20la%20pertenencia%20ª. (09 de Septiembre de 2020)

E-Healt Reporter. (2020). Credenciales digitales para proteger la privacidad de los ciudadanos. Revista Latinoamericana E-Health reporter. Tendencias. En colaboración con HIMSS. Recuperado de: https://ehealthreporter.com/es/noticia/credenciales-digitales-para-proteger-la-privacidad-de-los-ciudadanos/#. (08 de Septiembre de 2020)

Granryd, M. (2020). Covid-19: Digital identity can lead uso ut of lockdown, but user confidence is key. Grupo GSMA. Recuperado de: https://www.gsma.com/identity/covid-19-digital-identity-can-lead-us-out-of-lockdown-but-user-confidence-is-key. (08 de Septiembre de 2020)

Greuner, D. (2020). Certificados de inmunidad: Si debemos tenerlos, debemos hacerlo bien. Artículo de la Universidad de Harvard. Iniciativa de Impacto de respuesta rápida COVID-19. Recuperado de: https://ethics.harvard.edu/files/center-for-ethics/files/10immunity certificates.pdf

Hancock, A. (2020). La identificación digital debe estar diseñada para la privacidad y la equidad. Fundación Frontera Electrónica. Recuperado de: https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10. (08 de Septiembre de 2020)

Hardman, D. (2020). Una suave introducción a las credenciales verificables. Blog empresarial Evernym. Recuperado de: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/. (08 de Septiembre de 2020)

IFAI. (2011). Guía práctica para generar el aviso de privacidad. Instituto Federal de Acceso a la Información y Protección de Datos. Recuperado de http://inicio.ifai.org.mx/DocumentosdeInteres/privacidadguia.pdf. (09 de Septiembre de 2020)

Instituto Nacional Electoral INE. (2020). Acuerdo del consejo general del Instituto Nacional Electoral por el que se aprueba la expedición de constancias digitales de situación registral, como medida que promueva la identificación de las y los ciudadanos en sus trámites administrativos, con motivo de la declaratoria de emergencia sanitaria por la pandemia del Covid-19. Recuperado de: https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/113984/CGex202005-15-ap-4.pdf. (08 de Septiembre de 2020)

Ministerio de Comercio, Industria y Turismo, MINCIT. (2020). Artículo 15 de la Constitución Política de Colombia 1991. Recuperado de: https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-ycomunicacion/constitución-politica/derechos/articulo-15.aspx#:~:text=1991-,ART%C3%8DCULO%

2015%E2%80%94%20Todas%20las%20personas%20tienen%20derecho%20a%20su%20intimidad,debe%20respetarlos%20y%20hacerlos%20respetar. (09 de Septiembre de 2020)

Ministerio de las TIC. (2019). MINTIC. Diseño y medición- Indicador terminales por cada 100 habitantes. Recuperado de: https://colombiatic.mintic.gov.co/679/w3-article-74011.html. (10 de Septiembre de 2020)

Morris, N. (2020). 60 fuertes grupos de identidad soberana se enfocan en pasaportes y credenciales de inmunidad COVID-19. Noticias. Tecnología. Artículo. Recuperado de: https://ledger-insights.com/cargill-rabobank-trade-finance-enterprise-blockchain/. (08 de Septiembre de 2020)

Peeters, L., Parciak, T. & Walton, C. (2020). COVID-19 en personas con esclerosis múltiple: una iniciativa global de intercambio de datos. Revista de esclerosis múltiple. Artículo de investigación. Instituto de Investigación Biomédica e Instituto de Ciencia de Datos LM Peeter, Universidad de Hasselt, Agoralaan Building C, 3590 Diepenbeek, Bélgica. Recuperado de: https://journals.sagepub.com/doi/full/10.1177/1352458520941485. (08 de Septiembre de 2020)

Pueyo, X. (2020). Self-Sovereign Identity en la era de la pandemia: Validated ID se suma al Covid Credentials Initiative. Blog empresarial Validated ID. Recuperado de: https://www.validatedid.com/es/covid-credentials-initiative/. (08 de Septiembre de 2020)

Secretaria del Senado. (2020). Ley estatutaria 1266 de 2008. Diario oficial No. 47.219 de 31 de Diciembre de 2008. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. (09 de Septiembre de 2020).

Sistema Único de Información Normativa SUIN. (2009). Decreto 1727 de 2009. Recuperado de: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1338429. (09 de Septiembre de 2020)

Sistema Único de Información Normativa SUIN. (2010). Decreto 2952 de 2010. Recuperado de: http://www.suin-juriscol.gov.co/viewDocument.asp?id=1503907#:~:text=Que%20

dicha%20ley%20estatutaria%20tiene,el%20art%C3%ADculo%2015%20de%20la. (09 de Septiembre de 2020)

Song, W. Nohkbeh, R. Liau, D. (2020). Identidad soberana y control de la privacidad de usuarios para el rastreo de contactos. Biblioteca de la Universidad de Texas. Recuperado de: https://identity.utexas.edu/sites/default/files/202012/Self%20Sovereign%20Identity%20and%20User%20Control%20for%20Privacy-Preserving%20Contact%20Tracing.pdf

Unitag. (2020) ¿Qué es un código QR? Recuperado de: https://www.unitag.io/es/qrcode/what-is-a-qrcode. (17 de Septiembre de 2020)

World Wide Web. (2020). Modelo de datos para Credenciales Verificables 1.0. Expresar información verificable en la Web. Recuperado de: w3.org/TR/vc-data-model/#storage-providers-and-data-mining. (16 de Febrero de 2021)

Zaimova, R. (2020). Cómo combatir una crisis sanitaria como la del coronavirus con ayuda de los datos. Foro Económico Mundial WEFORUM. Desequilibrios económicos globales. Recuperado de: https://es.weforum.org/agenda/2020/04/como-combatir-una-crisis-sanitaria-como-la-del-coronavirus-con-ayuda-de-los-datos/. (09 de Septiembre de 2020)

Anexos

Anexo 1. Identificación de fuentes de información

Dentro del desarrollo del marco teórico del presente proyecto y los antecedentes utilizados a fin de contextualizar la situación problema, se identificación las fuentes de información más relevantes en las siguientes bibliotecas:

- Biblioteca Universidad de Harvard; Biblioteca Universidad de Texas

Las bases de datos utilizadas para la recolección de la información son:

- Fundación Frontera Electrónica; Instituto Federal de Acceso a la Información Y Protección de Datos IFAI; Instituto Nacional Electoral INE; Foro Económico Mundial ESFORUM

De igual manera se encuentran las siguientes revistas como fuentes de información recolectada

- Revista Covid Creeds
- Revista E - Health Reporter
- Revista GSMA
- Revista Evernym
- Revista de Investigación Médica SAGB Journals
- Revista Ledger Insights

Por último se encuentran los blogs empresariales de organizaciones pioneras en los campos de acción que funcionan como fuentes de información

- BTS ASSESSSORS
- Validated ID
- Unitag.io

Anexo 2. Análisis bibliométrico

2.1. Categorías

El material bibliográfico es organizado en las siguientes categorías en pro de realizar un manejo y lectura eficiente

- Credenciales de Identidad Digital
- Intercambio de datos global
- Uso de datos
- Iniciativa Credenciales Covid CCI
- Identidad Auto Soberana SSI
- Modelo tripartito de la verificación de datos
- Privacidad y equidad de datos

2.2. Palabras clave

Credencial digital, reactivación económica, privacidad, SSI Identidad auto soberana, cuarentena, identidad digital, recesión, uso de datos, Covid Creeds, nueva normalidad, credencial Covid, inmunidad de rebaño, pasaporte de inmunidad.

2.3. Documentos de referencia

2.3.1. Acuerdo para expedición de Constancias digitales, como medida que promueva la identificación de las y los ciudadanos en sus trámites administrativos, con motivo de la declaratoria de emergencia sanitaria por la pandemia del coronavirus, COVID-19.

Instituto Nacional Electoral INE. (2020). Recuperado de: https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/113984/CGex202005-15-ap-4.pdf. México

El documento estatal realiza un repaso acerca de los antecedentes que llevan a aprobar la expedición de constancias digitales con base a la declaratoria de emergencia sanitaria por COVID-19 a fin de identificar los ciudadanos en sus trámites administrativos, en función de preservar y promover los derechos fundamentales de cada individuo en el cual se encuentra la salud y la vida. Posteriormente analiza los motivos para aprobar la expedición de constancias

digitales entre los cuales se encuentran la suspensión de actividades, el privilegio al derecho de la salud y la consecución de los trámites propios de la entidad. Finalmente, se dan pasos en términos de diseño, vigencia, alcances, privacidad y seguridad de las constancias.

2.3.2. COVID-19 en personas con esclerosis múltiple: una iniciativa global de intercambio de datos

PEETERS, Liesbet; PARCIAK, Tina y WALTON Clare. Revista de esclerosis múltiple. SAGE Journals. Artículo de investigación. Recuperado de: https://journals.sagepub.com/doi/full/10.1177/1352458520941485. Bélgica

El artículo reflexiona la necesidad de obtener los suficientes datos de alta calidad que permitan evaluar la gravedad del COVID-19 en pacientes de Esclerosis Múltiple lo cual conlleva a analizar un enfoque de intercambio mundial de datos. El proceso implica una estrategia mundial en donde el intercambio de datos vislumbra una ventana hacia otros procesos de intercambio de datos global que permitan redefinir el rumbo de la pandemia, la reactivación social y el manejo de la enfermedad.

2.3.3. COVID 19: la identidad digital puede sacarnos del encierro, pero la confianza del usuario es clave

GRANRYD, Mats. Revista empresarial. Artículo asociación GSMA. Recuperado de: https://www.gsma.com/identity/covid-19-digital-identity-can-lead-us-out-of-lockdown-but-user-confidence-is-key. Latinoamérica

En este artículo se destaca la necesidad de utilizar la identidad digital de manera eficaz a fin de superar las medidas de distanciamiento social presente en todo el mundo. Se exaltan algunos mecanismos llevados a cabo por países como India y Corea del Sur que han aperturado en temas de selfies para cumplimiento de cuarentenas y verificaciones en línea de teléfonos para determinar relaciones interpersonales entre positivos para COVID-19. Representa la petición de Bill Gates para usar certificados digitales que indique quien ha sido probado, recuperado o administrado con alguna vacuna para el Virus. Termina identificando el papel central que tiene la industria móvil tanto en los avances que tiene para la iniciativa y en la lucha con la privacidad de los usuarios.

2.3.4. Credenciales digitales para proteger la privacidad de los ciudadanos

Revista Latinoamericana E-Health reporter. Tendencias. Recuperado de: https://ehealthreporter.com/es/noticia/credenciales-digitales-para-proteger-la-privacidad-de-los-ciudadanos/#. España.

El artículo comienza planteando la premisa de si las personas aceptaran la pérdida de su privacidad y la vigilancia de sus datos cuando el distanciamiento social sea levantado y se haya superado la pandemia; determinando las iniciativas de grandes empresas como Apple o Google para determinar positivos de COVID-19 por medio del bluetooth de los Smartphone y el uso de los datos privados por parte de los gobiernos. Finaliza destacando la importancia de la privacidad de las personas y como organizaciones como la Iniciativa de Credenciales COVID (CCI) se han enfocado en el desarrollo de credenciales verificables que involucren cuestiones de privacidad y ética de datos.

2.3.5. 60 fuertes grupos de identidad soberana se enfocan en pasaportes y credenciales de inmunidad COVID-19

MORRIS, Nicky. Artículo Ledger Insights. Tecnología. Recuperado de: https://ledger-insights.com/sovereign-identity-covid-19-immunity-passports-credentials/

Es un documento que destaca la "carrera" que muchas empresas han adoptado bajo la Iniciativa de Credenciales COVID (CCI) para utilizar la identidad digital como una estrategia que mitigue la propagación del virus y permita realizar una reapertura de sectores vitales dentro de cada Nación. Finaliza presentando las iniciativas de seguimiento para proteger la privacidad de los ciudadanos, enfocadas en los diversos proyectos a nivel global para hacer seguimiento a los casos COVID y el uso de herramientas tecnológicas avanzadas.

2.3.6. Una suave introducción a las credenciales verificables

HARDMAN, Daniel. Artículo en el blog de la empresa Evernym. Noticias de la empresa. Recuperado de: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/

El artículo comienza con la premisa de que las credenciales físicas que se utilizan como las licencias, pasaportes y boletos han hecho una transición hacia la digitalización y ahora pueden ser llevadas de manera práctica en Smartphone. Adicionalmente resalta el hecho de que la seguridad criptográfica actual hace de las credenciales digitales una identidad autónoma y multidimensional que proporciona a usuarios y organizaciones descentralización, flexibilidad y libertad.

2.3.7. Self-Sovereign Identity en la era de la pandemia: Validated ID se suma al Covid Credentials Initiative

PUEYO, Xavier. Artículo en el blog de la empresa Validated ID. Noticias y eventos. Recuperado de: https://www.validatedid.com/es/covid-credentials-initiative/

El artículo resalta el uso actual del contact-tracing manual para luchar contra la propagación de enfermedades infecciosas y su paso hacia un proceso automático debido al creciente número de infecciones y la pandemia por COVID-19. En adición a lo anterior, se resalta el uso del pasaporte inmunológico como medida para relajar las condiciones de confinamiento presentes a nivel global y robustecido con los picos de la pandemia y las nuevas variantes del virus encontradas. Finaliza invitando al público en general a unirse a la iniciativa del CCI aportando desde la experiencia personal y detectando los principales riesgos y vacíos presentes.

2.3.8. La identificación digital debe estar diseñada para la privacidad y la equidad

HANCOCK, Alexis. Artículo. Fundación Frontera Electrónica. EFF. Recuperado de: https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10

El documento hace un repaso por las exigencias que el mundo digital determina para que cada vez se verifique a las personas mediante su identidad digital y los posibles problemas en términos de privacidad y agravamiento de desigualdades sociales si dicha identificación no se diseña de manera correcta. Se enfatiza en el modelo tripartito de confianza entre emisor, titular y verificador para poseer un ecosistema de verificación de datos que permita realizar diversas actividades que la pandemia por COVID ha impedido.

2.3.9. Como combatir una crisis sanitaria como la del coronavirus con ayuda de los datos

ZAIMOVA, Rositsa. Artículo acerca de los desequilibrios globales del Covid-19. Foro Económico Mundial WEFORUM. Recuperado de: https://es.weforum.org/agenda/2020/04/como-combatir-una-crisis-sanitaria-como-la-del-coronavirus-con-ayuda-de-los-datos/

El artículo del Foro Económico Mundial contextualiza el problema de muchos países en donde las decisiones tomadas para hacer frente al COVID-19 no son las adecuadas por carecer de datos de calidad. Por lo anterior, se analizan las iniciativas de análisis de datos de teléfonos móviles en países como Bélgica en donde las tendencias de movilidad pudieron determinar los sitios que pueden presentar un foco del virus y por ende un posterior rebrote. Finaliza haciendo un análisis de la importancia de la privacidad de los datos bajo prácticas éticas y una legislación robusta de privacidad.

2.3.10. El pasaporte de inmunidad para acreditar el estado de salud a través de credenciales verificables y la blockchain

CALLIS, Silvia. Artículo en el blog empresarial BTC Assessors. Recuperado de: https://btcassessors.com/blog/el-pasaporte-de-inmunidad-para-acreditar-el-estado-de-salud-a-traves-de-credenciales-verificables-y-la-blockchain/

El documento del blog empresarial hace un recorrido por la evolución presente en las personas para sobrellevar los efectos que la pandemia ha traído y fundamentándose en la tecnología como medio de soluciones. Posteriormente realiza una introducción al pasaporte de inmunidad, su origen, las posibles soluciones que puede dar a efectos negativos de la pandemia y el modelo básico de confianza que debe conllevar. Finaliza hablando acerca de la importancia de la privacidad de los datos de los usuarios y la necesidad de generar una conciencia hacia el cambio digital.

2.3.11. Identidad soberana y control de usuarios para preserven la privacidad del rastreo de contactos

SONG, W. NOHKBEH, R. LIAU, D. Biblioteca de la Universidad de Texas. Recuperado de: https://identity.utexas.edu/sites/default/files/2020-12/Self%20Sovereign%20Identity%20and%20User%20Control%20for%20Privacy-Preserving%20Contact%20Tracing.pdf

El artículo Universitario comienza haciendo una introducción de los estragos que la pandemia por COVID-19 ha generado en la vida de las personas y las ordenes de confinamiento que gobiernos han impuesto para frenar la velocidad de contagia e impedir que se pierdan vidas. Aborda la alternativa de realizar un rastreo de contactos cercanos para casos positivos COVID y los problemas de privacidad que dicha alternativa conlleva. Posteriormente aborda la Identidad Auto Soberana ISS como una solución que transmite seguridad a los usuarios y eleva formas de otorgar solamente los datos necesarios para determinada interacción entre partes. Finaliza realizando un análisis de seguridad acerca del fraude y la confiabilidad del usuario.

2.3.12. Certificados de inmunidad: Si debemos tenerlos, debemos hacerlo bien

GREUNER, D. Artículo de la Universidad de Harvard. Iniciativa de Impacto de respuesta rápida COVID-19. Recuperado de: https://ethics.harvard.edu/files/center-for-ethics/files/10immunitycertificates.pdf

El artículo científico de la Universidad de Harvard presenta un documento bajo principios éticos de la importancia que tiene el correcto manejo de los datos para la realización de certificados de inmunidad orientados a reactivar los países económicamente y lograr una nueva normalidad coordinada y segura. El artículo hace un repaso acerca de la arquitectura necesaria

para la privacidad y la implementación de la equidad y protección de las libertades civiles. Finaliza concluyendo los pasos que se deben tener en cuenta a futuro y la utilidad de los certificados de inmunidad sin dejar de lado que preservar la salud pública no tiene por qué afectar o comprometer los derechos personales.

2.4. Tabla comparativa

Tabla 2. Tabla comparativa de fuentes de información

Titulo	Metodología y supuestos	Uso de la tecnología	Conclusiones y aportes
1. Acuerdo para expedición de Constancias Digitales, como medida que promueva la identificación de las y los ciudadanos en sus trámites administrativos, con motivo de la declaratoria de emergencia sanitaria por la pandemia del coronavirus, Covid-19. "Contexto Internacional"	El documento estatal revisa los antecedentes de la evolución de la emergencia sanitaria por COVID-19 y determina la viabilidad del uso de Credenciales Digitales a fin de ofrecer una alternativa para la consecución de las actividades propias de la entidad y salvaguardar la salud y vida de funcionarios y ciudadanía en general.	Presenta un diseño para la constancia digital en formato PDF con datos principales del usuario. Establece un flujo de actividades para la solicitud, verificación y posterior envío de la credencial bajo diversos canales. Determina incluir en las constancias digitales los códigos QR que identificaran su lectura y veracidad.	Aprueba la expedición de Constancias digitales para promover la identificación en los ciudadanos en sus trámites administrativos y demuestra avances para reactivar los sectores más influyentes dentro de cada Nación que han sido afectados por la COVID-19 a través de las Constancias Digitales.
2. COVID-19 en personas con esclerosis múltiple: una iniciativa global	El artículo se enfoca en comprender los efectos del COVID-19 en los pacientes con dicha enfermedad y retroalimentar dichos resultados a los profesionales de la salud	Establece la importancia de crear grupos de trabajo interdisciplinarios dedicados a reunir	Promueve la formulación de estrategias globales de recolección de datos y destaca que puede ser utilizado como una plantilla para que diversas partes trabajen juntas a escala

de intercambio de datos "Contexto Internacional"	durante la pandemia; para lo anterior, diseña un enfoque en el cual la implementación del conjunto de datos centrales de COVID-19 de diversos registros permite generar una plataforma global confiable de datos y resultados.	conjuntos de datos básicos de COVID-19. Determina la necesidad de establecer plataformas o medios que permitan canalizar de manera eficiente los datos de COVID-19 a escala global.	internacional fuera del alcance de la crisis por COVID-19.
3. COVID 19: la identidad digital puede sacarnos del encierro, pero la confianza del usuario es clave "Contexto Nacional"	Destaca la importancia de la identidad digital para sobreponerse ante las medidas de distanciamiento social y el creciente uso de los sistemas y servicios bajo acceso remoto. Genera la premisa de la privacidad de los usuarios y su confiabilidad como posibles barreras para la puesta en marcha del proyecto	Determina el uso de la industria móvil como elemento principal para el manejo de las credenciales digitales y su uso generalizado en el mundo. Organiza la identidad digital como una infraestructura pública que se puede aprovechar para recuperarse de las consecuencias de la pandemia y estar más preparadas para la siguiente.	Establece la dualidad entre la importancia de las identidades digitales para sobreponerse al distanciamiento social que ha provocado la pandemia y la priorización de la privacidad de los usuarios y su confianza para el trámite a nivel global de sus datos personales.
4. Credenciales digitales para proteger la privacidad de los ciudadanos "Contexto Internacional"	Establece la Iniciativa de Credenciales COVID (CCI) como una alternativa de solución para poder controlar la propagación de la pandemia y comprobar qué ciudadanos han sido testados o recibieron la vacuna.	Establece el uso de Credenciales Verificables VC como herramienta segura para guardar información sensible y valiosa que permita salvaguardar los datos de sus usuarios.	Establece las Credenciales Verificables como la herramienta que permitirá realizar una apertura mundial es diversos contextos y salvaguardar la privacidad y datos de los ciudadanos. Enfatiza en que es momento de pensar en la identidad digital

		Resalta el papel de la tecnología y su principal uso en la tarea de facilitar los procesos para que cualquier individuo sea capaz de manejar su propia VC.	como un valor agregado para las personas e instituciones simular a la infraestructura.
5. 60 fuertes grupos de identidad soberana se enfocan en pasaportes y credenciales de inmunidad COVID-19 “Contexto Internacional”	Destaca la fuerte movilización de organizaciones hacia un conglomerado que establece el uso de credenciales de inmunidad por COVID-19 y su uso tanto para pruebas, vacunas y seguimiento de personas.	Prioriza el uso de elementos tecnológicos como la ubicación GPS para el seguimiento de personas. Establece el uso del Bluetooth como una forma de determinar las personas que pasaron cerca de un positivo COVID en un momento determinado y así realizar cercos epidemiológicos más eficientes	El documento demuestra que aunque el enfoque de la Iniciativa de Credenciales COVID sea el uso de Certificados Verificables para demostrar que u individuo ha recibido la vacuna; su uso temprano puede derivar en el aprovechamiento de recursos para realizar cercos epidemiológicos y comprobación de resultados de pruebas.
6. Una suave introducción a las credenciales verificables “Contexto Internacional”	Subraya la importancia de la transición en las credenciales hacia la digitalización y su robusta seguridad a través de las características criptográficas facilitando la interacción entre usuarios, dando apertura al crecimiento económico e impulsando la labor de las organizaciones.	Presenta el modelo de datos de credenciales verificables del W3C en donde se presenta un modelo tripartito de confianza entre emisores, titulares y verificadores.	Las Credenciales de Identidad Digital conllevan una serie de beneficios para empresas, gobiernos y usuarios. Los usuarios tendrán interacción constante con el mundo digital, los gobiernos tendrán oportunidad para crecimiento económico y las empresas automatizaran trabajo mejorando su eficiencia.

7. Self-Sovereign Identity en la era de la pandemia: Validated ID se suma al Covid Credentials Initiative "Contexto Internacional"	Destaca el enfoque que la Iniciativa de Credenciales COVID (CCI) ha tenido en pro de salvaguardar la Identidad Auto Soberana y proteger la privacidad de los usuarios estableciendo una red local de confianza y una prueba de inmunidad para reactivación general.	Utiliza el contact-tracing automático para luchar contra la propagación a través de los cercos epidemiológicos. Destaca el uso de las credenciales verificables para asegurar que la fuerza laboral sean libres de portar el COVID-19	Determina que en un mundo donde la privacidad está cada vez más condicionada, es importante que la Identidad Auto Soberana propia de las Credenciales Digitales sea un enfoque defendido sin caer en el error de privilegiar a aquellos que tengan sistemas inmunológicos elevados.
8. La identificación digital debe estar diseñada para la privacidad y la equidad "Contexto Internacional"	Las credenciales verificables representan afirmaciones digitales en las que confían tres partes, el emisor, el verificador y el titular de la misma. Las VC basan su utilidad en las pruebas de conocimiento cero que son valores criptográficos en los cuales solo se presenta la información que solicitan, sin acceder a otro tipo de datos	Modelo tripartito de confianza para verificación de datos (Emisor – Titular – Verificador)	Las soluciones para hacer que la información personal sea fácil de compartir no debe traspasar el límite de la protección de datos o la falta de acceso a la tecnología.
9. Como combatir una crisis sanitaria como la del coronavirus con ayuda de los datos "Contexto Internacional"	Las medidas de los funcionarios de sanidad de cada país influirán en el número de personas que morirán. El análisis de datos de telefonía móvil puede prever las tendencias humanas y responder ante futuras crisis sectoriales.	Utiliza el análisis de datos contextual (sector, región, país o global) para tomar decisiones que permitan contrarrestar los efectos del COVID-19.	La utilización y análisis de datos puede permitir que los gobiernos se preparen mejor para hacer frente a las consecuencias del COVID-19 pero la privacidad de los datos es un ítem que debe ser respetado a través de las practicas éticas idóneas.
10. El pasaporte de inmunidad para acreditar el	La identidad auto-soberana junto con la blockchain, permiten crear identidades digitales para	La blockchain como infraestructura idónea	El pasaporte de inmunidad puede recoger la información relevante en términos de esta

estado de salud a través de credenciales verificables y la blockchain "Contexto Nacional"	la gestión de los pasaportes de identidad, sin dañar la propia privacidad del individuo.	para la identidad descentralizada.	pandemia y futuras y ayudar a preparar al mundo para una activación de diversos sectores de forma rápida y ordenada.
11. Identidad soberana y control de usuarios para preserven la privacidad del rastreo de contactos "Contexto Internacional"	Los usuarios deben ser los únicos propietarios de sus datos de diagnóstico para esta y futuras pandemias. Los modelos de rastreo de contactos bajo la ISS ayudan a detener la propagación de COVID-19 y protegen la privacidad de la información del usuario pues este último puede elegir cuanta información compartir	Puesta en marcha de la aplicación en 6 pasos 1. Registro 2. Configuración de colección de contactos 3. Recogida de contactos 4. Configuración de Notificación de contacto 5. Informe de prueba COVID 6. Notificación de contacto	Con los avances de la pandemia y los esfuerzos para detener su avance, el rastreo de contactos positivos se ha vuelto una opción viable que solo puede ser soportada bajo la visión de la Identidad Auto Soberana, la cual funciona como el elemento vital para salvaguardar los datos personales de los usuarios.
12. Certificados de inmunidad: Si debemos tenerlos, debemos hacerlo bien "Contexto Internacional"	Preservar la salud pública no tiene por qué comprometer los derechos personales de los individuos. Los certificados de inmunidad pueden revertir las consecuencias económicas y sociales del COVID-19	Los certificados digitales de inmunidad son la nueva fuente de información que los funcionarios de salud pública y los gobiernos necesitan para avanzar y recuperarse.	El uso de certificados digitales plantea preocupaciones sobre la equidad y libertad civil que debe cuidarse con recelo bajo legislaciones fuertes

Fuente: Elaboración propia en función de las fuentes de información consultadas, 2020.

Anexo 3. Elaboración de meta-análisis

Introducción

A continuación se presenta la elaboración del meta-análisis de los documentos utilizados como referencia, extraídos de fuentes de contextos nacionales e

internacionales y en los cuales se identificaron aspectos metodológicos, conclusiones y aportes de los documentos. Todo lo anterior trabaja en función de determinar las ideas más relevantes que determinen el desarrollo de Credenciales Digitales como estrategia de aplicación en Colombia.

Clasificación de las categorías de análisis

Para llevar a cabo los análisis comparativos, se clasificaron en categorías los documentos que fueron utilizados y que determinaran los puntos centrales del proyecto así:

- Credenciales de Identidad Digital
- Intercambio de datos global
- Iniciativa Credenciales Covid
- Identidad Auto Soberana
- Modelo tripartito de la verificación de datos

3.1. Análisis comparativo desde la metodología

- Credenciales de Identidad Digital

1. Acuerdo para expedición de Constancias Digitales, como medida que promueva la identificación de las y los ciudadanos en sus trámites administrativos, con motivo de la declaratoria de emergencia sanitaria por la pandemia del coronavirus, Covid-19.	Comparación En los tres documentos se llega al acuerdo de que la identidad digital puede ayudar a mitigar las consecuencias que las medidas de distanciamiento social han traído para cada contexto de las naciones y por lo tanto debe ser redirigido para entender que está equiparado con la infraestructura que se cuenta en una organización. Dentro de los documentos se encuentran referencias hacía el modelo de credenciales verificables de la W3C que presenta un robusto trabajo en términos de organización, seguridad, mecanismos, ensamble y puesta en marcha.
3. COVID 19: la identidad digital puede sacarnos del encierro, pero la confianza del usuario es clave	
6. Una suave introducción a las credenciales verificables	

- Intercambio de datos global

2. COVID-19 en personas con esclerosis múltiple: una iniciativa global de intercambio de datos	Comparación Los documentos instan al lector a entender la necesidad de crear un sistema en el que diversos grupos de trabajo se orienten a reunir datos COVID-19 y el trabajo que organizaciones como la de telefonía móvil (La cual conoce de mejor manera todos los datos y ubicaciones de los usuarios) puede desarrollar o aportar en marcos de datos para articular de manera adecuadas los procesos que se buscan desarrollar.
9. Como combatir una crisis sanitaria como la del coronavirus con ayuda de los datos	

- Iniciativa Credenciales COVID

4. Credenciales digitales para proteger la privacidad de los ciudadanos	Comparación Los documentos concuerdan en ideas como los son la orientación de diversos conglomerados de organizaciones a nivel mundial para implementar la iniciativa de credenciales COVID CCI y cómo esta iniciativa puede ser usada en etapas tempranas para destacar información de pruebas, seguimientos de contactos, hasta una fase futura de vacunas y certificados de las mismas. Adicionalmente, analiza la importancia de contar con un sistema que garantice que cada individuo sea capaz de manejar su propia información bajo el uso de la tecnología y con un componente de privacidad de datos
5. 60 fuertes grupos de identidad soberana se enfocan en pasaportes y credenciales de inmunidad COVID-19	

- Identidad Auto Soberana

7. Self-Sovereign Identity en la era de la pandemia: Validated ID se suma al Covid Credentials Initiative	Comparación Los tres documentos concuerdan en la ISS Identidad Auto Soberana como la herramienta para proteger la privacidad de los usuarios ayudando a detener la propagación de COVID-19 bajo la premisa básica que preservar la salud pública y que aún en una pandemia global no se pueden sobrepasar los derechos personales de los individuos, en este caso el de la privacidad y manejo de sus datos sensibles.
11. Identidad soberana y control de usuarios para preserven la privacidad del rastreo de contactos	
12. Certificados de inmunidad: Si debemos tenerlos, debemos hacerlo bien	

- Modelo tripartito de la verificación de datos

<table>
<tr><td>8. La identificación digital debe estar diseñada para la privacidad y la equidad</td><td rowspan="2">Comparación
Los documentos basan sus premisas en el modelo W3C que incluye un modelo tripartito de confianza en el que interactúa emisor, titular y verificador de las certificaciones digitales. Adicionalmente muestran su utilidad al determinar que entre partes se pueden compartir solo la información solicitada, en donde el emisor no pierde su capacidad de manejar los datos que posee y los verificadores no acceden a más información de la netamente necesaria.</td></tr>
<tr><td>10. El pasaporte de inmunidad para acreditar el estado de salud a través de credenciales verificables y la blockchain</td></tr>
</table>

3.2. Análisis comparativo desde las conclusiones y aportes

- Credenciales de Identidad Digital

1. Acuerdo para expedición de Constancias Digitales, como medida que promueva la identificación de las y los ciudadanos en sus trámites administrativos, con motivo de la declaratoria de emergencia sanitaria por la pandemia del coronavirus, Covid-19.	Comparación Los tres documentos concluyen que es importe hacer una transición de las certificaciones físicas hacia las certificaciones digitales demostrando que cada vez es más necesario que los individuos estén relacionados con el mundo digital y a su vez obtengan los beneficios que dicho elemento genera en los usuarios. Adicionalmente se hace gran énfasis en la confianza del usuario para permitir poner en práctica dichos elementos, sin ignorar la responsabilidad existente con la defensa de la privacidad de los datos de los mismo y el trabajo creciente para asegurar que la seguridad de las certificaciones digitales este a tal punto que evite las vulneraciones, fuga de datos y suplantación de información.
3. COVID 19: la identidad digital puede sacarnos del encierro, pero la confianza del usuario es clave	
6. Una suave introducción a las credenciales verificables	

- Intercambio de datos global

2. COVID-19 en personas con esclerosis múltiple: una iniciativa global de intercambio de datos	Comparación Ambos documentos resaltan la importancia del manejo de los datos como estrategia para solventar crisis asociadas a la pandemia y diversas problemáticas presente en el mundo. El foro Económico Mundial hace especial énfasis en la utilidad del manejo de los datos para conocer las tendencias que tienen las personas y así obtener una visión de los focos principales de cada región. La revista médica otorga un avance importante en la unión de grupos de trabajos para reunir datos referentes a la pandemia y su efecto dentro de otras enfermedades, lo cual no solo representa un avance médico y tecnológico sino que además deriva en una ventana con vista a los múltiples beneficios que el manejo de datos a nivel global
9. Como combatir una crisis sanitaria como la del coronavirus con ayuda de los datos	

	tiene para combatir o mitigar los problemas asociados a la pandemia.

- Iniciativa Credenciales COVID

4. Credenciales digitales para proteger la privacidad de los ciudadanos	Comparación A primera vista la Iniciativa Credenciales COVID se concluye como el proyecto central para ayudar a reactivar los contextos primordiales de cada región y devolverle una normalidad transitoria a la humanidad; no obstante, se demuestra cómo una vez más la unión de diversos conglomerados puede derivar en iniciativas de éxito para ayudar a mejorar la calidad de vida de las personas. De igual manera, ambos documentos concluyen en la importancia de manejar modelos estandarizados envueltos en componentes éticos cuyo objetivo principal sea proteger y promover la privacidad de los datos de los usuarios a toda costa.
5. 60 fuertes grupos de identidad soberana se enfocan en pasaportes y credenciales de inmunidad COVID-19	

- Identidad Auto Soberana

7. Self-Sovereign Identity en la era de la pandemia: Validated ID se suma al Covid Credentials Initiative	Comparación Se concluye que aún en medio de una pandemia, el derecho a la salud se encuentra por debajo de otros derechos como la privacidad y el bienestar personal. Por lo tanto, en medio de la constante aparición de proyectos para seguimiento de contactos, utilización de elementos de GPS, datos privados, contactos, eventos y demás, es necesario contar con un sistema que garantice que las personas y por lo tanto usuarios sigan contando con la capacidad intransferible de manejar sus propios datos y en especial aquellos que son de carácter sensible. La Identidad Auto Soberana ISS se vislumbra entonces como la solución para que las certificaciones digitales
11. Identidad soberana y control de usuarios para preserven la privacidad del rastreo de contactos	
12. Certificados de inmunidad: Si debemos tenerlos, debemos hacerlo bien	

	sean una realidad dentro de los términos éticos necesarios.

- Modelo tripartito de la verificación de datos

8. La identificación digital debe estar diseñada para la privacidad y la equidad	Comparación Se concluye que se debe hacer avances en el modelo de la W3C para las Credenciales Verificables en donde intervienen los 3 elementos de la verificación de datos (Emisor/Titular/Verificador) y que cuenta con ítems especiales como lo son la seguridad criptográfica con códigos QR; los avances en temas de privacidad y seguridad y los alcances de las CV. De igual manera, se definen los alcances que cada uno de los actores del modelo tripartito tienen dentro de la verificación de los datos y la utilidad de las certificaciones o credenciales digitales para su aplicabilidad no solo durante la pandemia sino para la sistematización de diversos elementos del diario vivir.
10. El pasaporte de inmunidad para acreditar el estado de salud a través de credenciales verificables y la blockchain	