

Acreditación Institucional
de Alta Calidad Educativa

Doctorado en Informática

Modelos avanzados de privacidad y seguridad para la gestión de identidades digitales descentralizadas basadas en Blockchain y Criptografía de Conocimiento Cero

Cristian Adrián Pazmiño Cortez

Director: Dr. Rodrigo Cadena Martínez

Quito, Ecuador, 30 de abril de 2026

Universidad Americana de Europa (ROR: https://ror.org/03698ym41)

Resumen

La presente investigación evaluó, de forma comparativa, un modelo avanzado de identidad digital descentralizada que combina blockchain, pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo. Su propósito era verificar si esa combinación fortalece la privacidad, la seguridad, la interoperabilidad y la soberanía digital del usuario frente a las alternativas que ya existen. El estudio adoptó un enfoque mixto, aplicado y tecnológico, con un diseño cuasi-experimental pensado para poner el modelo a prueba de manera empírica y no solo teórica. La validación tuvo lugar en un entorno de simulación controlada, donde la investigación comparó cuatro esquemas de gestión de identidad: el centralizado de siempre, un modelo básico de identidad autosoberana, ese mismo modelo con pruebas de conocimiento cero añadidas, y el modelo que se propone en esta tesis. Como base de comparación, el estudio utilizó indicadores técnicos y normativos: latencia, tamaño de la prueba criptográfica, porcentaje de atributos divulgados, índice de no vinculabilidad, cumplimiento normativo, seguridad y usabilidad. Los resultados, en general, favorecen al modelo propuesto: este divulga menos atributos, mejora la no vinculabilidad y se ajusta mejor al RGPD, al eIDAS 2.0 y a la norma ISO/IEC 29100. La excepción es la latencia, algo mayor que en los demás modelos; un costo razonable frente a lo que se gana en privacidad y cumplimiento normativo. El control de acceso adaptativo, por su parte, refuerza la seguridad sin afectar de forma notable la usabilidad percibida por el usuario. Estos hallazgos indican que integrar blockchain, pruebas de conocimiento cero, cifrado homomórfico y políticas ABAC constituye una vía viable para proteger datos personales, y avanzar hacia sistemas de identidad digital más seguros y centrados en el usuario.

Palabras clave: identidad digital descentralizada, blockchain, pruebas de conocimiento cero, privacidad, soberanía digital.

Abstract

This research aimed to evaluate an advanced decentralized digital identity model that combines blockchain, zero-knowledge proofs, homomorphic encryption, and adaptive access control to enhance user privacy, security, interoperability, and digital sovereignty. The methodology is mixed, applied, and technological in nature, with a quasi-experimental approach based on empirical validation. A controlled environment was developed through simulations and laboratory tests, comparing four identity management models: a conventional centralized model, a basic self-sovereign identity model, a self-sovereign identity model with zero-knowledge proofs, and the proposed model. The technical and regulatory aspects of the model were evaluated, including latency, cryptographic proof size, percentage of disclosed attributes, unlinkability index, regulatory compliance, security, and usability. The results indicate that the proposed model involves less attribute disclosure, achieves greater unlinkability, and provides better compliance with GDPR, eIDAS 2.0, and ISO/IEC 29100 for the user, although it still presents operational latency. In addition, adaptive access control improved security without negatively affecting usability. In conclusion, blockchain as a trust anchor, zero-knowledge proofs, homomorphic encryption, and ABAC policies are beneficial for protecting personal data, reducing correlation risks, and promoting more secure, interoperable, and user-centered digital identity models.

Keywords: decentralized digital identity, blockchain, zero-knowledge proofs, privacy, digital sovereignty.

Dedicatorias

Dedico este estudio, ante todo, gracias a Dios; él me ha dado vida, salud, sabiduría y fuerza para progresar en este estudio. Me ha guiado cuando he estado cansado, cuando mi vida se ha vuelto un caos, pero con fe, disciplina y la creencia de que todo esto es para mí. A mi esposa, por su paciencia, comprensión y por estar ahí para mí, toda mi vida. Gracias por estar presente en todas las etapas del trabajo que realizo y por entender las largas horas de estudio, investigación y trabajo, y por siempre darme ánimo cuando me sentía cansado y no podía continuar. Tu apoyo siempre me ha proporcionado la fuerza para seguir preparándome, aprender y continuar. A mi hija, una de mis mayores inspiraciones y quien me motiva a ser mejor cada día. Esta victoria también es para ella porque es quien tengo y me recuerda que podemos construir un futuro haciendo lo que necesitamos con esfuerzo, responsabilidad y ejemplo. Que este trabajo sea el mejor del que podamos estar orgullosos, de poder lograr grandes cosas gracias a nuestra dedicación y aprendizaje y al conocimiento que necesitamos.

Agradecimientos

Mis padres han sido maravillosos al enseñarme mucho sobre valores, responsabilidad y una pasión por el aprendizaje. Muchas gracias por una buena educación, por mostrarme cómo el trabajo duro, la honestidad y la perseverancia importan, y por inculcarme un deseo ardiente de ser mejor. A mi esposa e hija, quienes han sido mi mayor apoyo emocional y motivación para seguir preparándome. Gracias por la paciencia, comprensión y amor durante el tiempo, esfuerzo y sacrificios tanto de estudio como de investigación. Fue una gran bendición para mí contar con la Universidad Americana de Europa para proporcionarme el espacio académico y formativo para contribuir a esta investigación de doctorado. Al Dr. Rodrigo Cadena Martínez, director de la tesis, por su orientación y apoyo y sus perspicaces ideas para este trabajo que contribuyeron tanto al desarrollo académico, metodológico y científico de esta investigación. A los profesores del programa de Doctorado en Informática por el apoyo a los estudiantes en la preparación de conocimientos y experiencia y la investigación y el desarrollo de una teoría de investigación en el contexto de los desafíos actuales en informática, seguridad de la información y transformación digital.

Contenido

Resumen ii

Abstract iii

Dedicatorias iv

Agradecimientos v

Contenido vi

Introducción 1

1. Problema de investigación 4

1.1. Problema 4

1.2. Justificación 5

1.3. Objetivo 6

1.4. Hipótesis o Supuesto Hipotético 6

1.5. Variables o Categoría de análisis 7

2. Estado del arte, antecedentes y marco teórico-conceptual integrado 9

2.1. Estado del Arte 9

2.2. Síntesis crítica del estado del arte 11

2.3. Evolución Histórica de la Identidad Digital 13

2.4. Protocolos y Tecnologías Fundamentales en Identidad Digital Descentralizada 16

2.5. Plataformas y Proyectos Relevantes en Identidad Digital Descentralizada 20

2.6. Retos y limitaciones en la identidad digital descentralizada 31

2.7. Investigaciones recientes vinculadas al estado del arte 34

2.8. Brechas de conocimiento derivadas del estado del arte 38

2.9. Síntesis integradora del estado del arte 40

2.10. Aportes teóricos, metodológicos y normativos derivados del estado del arte 41

2.11. Implicaciones del estado del arte para el modelo propuesto 44

2.12. Marco teórico-conceptual integrado 45

2.13. Marco histórico 48

2.14. Marco referencial 51

2.15. Marco legal 54

2.16. Categorías conceptuales para la operacionalización 57

2.17. Conexión metodológica, brechas y proyección investigativa 60

3. Propuesta metodológica 61

3.1. Enfoque metodológico 61

3.2. Diseño de la investigación 63

3.3. Nivel de investigación 68

3.4. Métodos y técnicas 68

3.5. Validez y confiabilidad 70

3.6. Innovación metodológica 71

3.7. Población y muestra 71

3.8. Correspondencia entre marco teórico, variables e indicadores de medición 73

3.9. Instrumentos, validación y procedimiento de aplicación 75

3.10. Criterios de selección de los modelos comparados 82

3.11. Matriz de consistencia metodológica 83

3.12. Validación del modelo propuesto mediante juicio de expertos 84

4. Resultados y Discusión 84

4.1. Resultados del objetivo general 84

4.2. Resultados por objetivos específicos 91

4.3. Discusión de resultados frente al estado del arte 96

5. Conclusiones, recomendaciones, limitaciones y desafíos 100

5.1. Limitaciones y desafíos 100

5.2. Conclusiones y recomendaciones 100

Referencias 104

Glosario 111

Anexo A. Instrumento propuesto (opcional, no aplicado) para la validación del modelo mediante juicio de expertos 113

Lista de tablas y figuras

Tablas

Tabla 1. Variables Independientes 7

Tabla 2. Variables Dependientes 7

Tabla 3. Variables de Control 8

Tabla 4. Criterios de construcción del estado del arte 9

Tabla 5. Brechas de conocimiento derivadas del estado del arte 38

Tabla 6. Articulación entre brechas de conocimiento 39

Tabla 7. Fuentes documentales e indicadores aplicados en el análisis documental 70

Tabla 8. Contraste de la hipótesis general por dimensiones evaluadas 74

Tabla 9. Matriz de Variables 78

Tabla 10. Criterios de selección de los modelos comparados 82

Tabla 11. Matriz de consistencia metodológica 83

Tabla 12. Significancia de diferencias entre sistemas (ANOVA). 92

Tabla 13. Mejora relativa de la propuesta frente a un sistema centralizado. 92

Tabla 14. Cumplimiento relativo por estándar/marco. 93

Tabla 15. Matriz de riesgos comparativa (nivel cualitativo). 94

Tabla 16. Resultados comparativos (media ± DE) por sistema (n=120 ejecuciones/sistema). 95

Tabla 17. Variables Cubiertas 99

Tabla 18. Glosario de términos 111

Tabla 19. Instrumento propuesto de validación por juicio de expertos 114

Figuras

Figura 1. Latencia de autenticación (IC 95%). 85

Figura 2. Exposición de datos (IC 95%). 87

Figura 3. Comparación multicriterio (0–100). 89

Figura 4. Matriz de correlación. 91

Introducción

La gestión de la identidad digital es hoy uno de los desafíos más importantes de la transformación digital, sencillamente porque buena parte de lo que hacemos —trámites gubernamentales, estudios, finanzas, vida social— depende de poder autenticar, autorizar y verificar atributos personales de forma confiable. Tradicionalmente esto lo ha manejado una entidad central: pública, privada o corporativa, que guarda y controla las credenciales del usuario. Ese modelo permitió que los servicios digitales crecieran rápido, pero trajo consigo riesgos que ya conocemos bien: concentración de datos, suplantación de identidad, robo de credenciales, exposición innecesaria de información personal y, en el fondo, la pérdida del control del usuario sobre sus propios datos (Mühle et al., 2018).

Como respuesta han aparecido los modelos de identidad digital descentralizada e identidad autosoberana, que buscan devolverle al usuario el control de sus credenciales mediante identificadores descentralizados, credenciales verificables y tecnologías de registro distribuido. Es un avance real frente a los sistemas centralizados: baja la dependencia de terceros y facilita que las credenciales se puedan llevar de un servicio a otro. Pero todavía arrastra problemas de privacidad, interoperabilidad, escalabilidad, revocación, cumplimiento normativo y protección frente a ataques de correlación. En particular, la transparencia propia de algunas arquitecturas blockchain puede dejar expuestos metadatos o patrones de interacción que terminan comprometiendo la no vinculabilidad de las identidades digitales (Goodell & Aste, 2019; Reece et al., 2022).

El problema de fondo que aborda esta investigación es que ni los modelos centralizados ni los descentralizados básicos resuelven del todo la tensión entre verificabilidad, privacidad, seguridad, interoperabilidad y soberanía digital. Los centralizados son eficientes, pero

concentran el riesgo; los autosoberanos básicos mejoran el control del usuario, pero pueden seguir siendo vulnerables a la correlación de transacciones, a la exposición de atributos y a la falta de mecanismos de acceso adaptativos. Por eso hace falta evaluar arquitecturas más avanzadas, capaces de combinar mecanismos criptográficos y políticas dinámicas que reduzcan la exposición de datos personales sin sacrificar la funcionalidad del sistema.

Aquí entran en juego varias piezas: las pruebas de conocimiento cero permiten verificar un atributo sin revelar información sensible; el cifrado homomórfico permite operar sobre datos cifrados sin descifrarlos; blockchain puede servir de ancla de confianza y trazabilidad; y el control de acceso adaptativo basado en atributos permite decidir autorizaciones según el contexto, el riesgo y las políticas de seguridad vigentes. Juntar estas piezas abre la posibilidad de construir un modelo de identidad digital descentralizada más robusto, que proteja mejor la privacidad, fortalezca la seguridad, mejore la interoperabilidad y le devuelva soberanía digital al usuario (Schanzenbach et al., 2019; Zhou et al., 2020; Hu et al., 2015).

En consecuencia, el objetivo general de esta investigación es evaluar comparativamente, mediante un diseño cuasi-experimental, un modelo avanzado de identidad digital descentralizada que integra blockchain, pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo, con el fin de determinar su impacto en la privacidad, la seguridad, la interoperabilidad, la usabilidad y la soberanía digital frente a modelos tradicionales y modelos de identidad autosoberana existentes. Para ello, se desarrolla una evaluación basada en simulación controlada, métricas técnicas, indicadores normativos y comparación entre cuatro configuraciones de gestión de identidad: modelo centralizado tradicional, modelo SSI básico, modelo SSI con pruebas de conocimiento cero y modelo propuesto.

El aporte principal de esta tesis es proponer y validar una arquitectura integrada, donde blockchain, ZKP, cifrado homomórfico y ABAC no se estudian por separado, sino como piezas articuladas de un modelo que se puede evaluar empíricamente. Con eso se va más allá de una simple revisión descriptiva del estado del arte: se ofrece evidencia comparativa sobre cuánto se reduce la divulgación de atributos, cuánto mejora la no vinculabilidad, cuánto sube el cumplimiento normativo y cómo se fortalece la seguridad sin dañar seriamente la usabilidad. En ese sentido, la tesis deja una base metodológica y tecnológica para diseñar sistemas de identidad digital descentralizada más seguros, interoperables, verificables y centrados en el usuario.

La investigación se estructura en cinco capítulos. El primer capítulo presenta el problema de investigación, la justificación, los objetivos, la hipótesis general y las variables de análisis. El segundo capítulo desarrolla el estado del arte y el marco teórico-conceptual, identificando las principales brechas de conocimiento que justifican el modelo propuesto. El tercer capítulo expone la propuesta metodológica, el diseño cuasi-experimental, la población tecnológica, las variables, los indicadores y el procedimiento de validación. El cuarto capítulo presenta los resultados y la discusión frente al estado del arte. Finalmente, el quinto capítulo recoge las conclusiones, recomendaciones, limitaciones y desafíos derivados de la investigación.

1. Problema de investigación

1.1. Problema

La transformación digital multiplicó el uso de identidades digitales: hoy se usan para transacciones financieras, trámites gubernamentales y buena parte de la vida social en línea. El problema es que los modelos centralizados que todavía dominan este espacio —donde un tercero administra los datos personales— arrastran varias vulnerabilidades serias:

- La concentración de datos sensibles en un solo lugar, que los vuelve un blanco atractivo para ciberataques masivos (Mühle et al., 2018).
- Suplantación de identidad y robo de credenciales, casi siempre vía phishing o brechas de seguridad (Zhou et al., 2020).
- Una exposición de información mayor de la necesaria cuando se verifican atributos (Reece et al., 2022).
- Y, de fondo, la falta de soberanía del usuario sobre sus propias credenciales y su portabilidad (Goodell & Aste, 2019).

Como respuesta a esto han aparecido la identidad digital descentralizada (Decentralized Identifiers – DID) y la identidad autosoberana (SSI), que le devuelven al usuario la propiedad, el control y la portabilidad de sus credenciales apoyándose en blockchain y credenciales verificables (Schanzenbach et al., 2019). Aun así, llevarlas a una adopción masiva no es sencillo:

La transparencia propia de blockchain puede facilitar que se correlacionen identidades, comprometiendo la privacidad.

Los mecanismos actuales de autenticación y autorización no siempre bastan para proteger datos sensibles.

Falta de modelos adaptativos de control de acceso para entornos distribuidos y dinámicos.

Y, además, la necesidad de cumplir normativas globales como el RGPD y el eIDAS 2.0.

De ahí que tenga sentido pensar en un modelo híbrido que junte tecnologías más avanzadas —pruebas de conocimiento cero (ZKP), cifrado homomórfico y políticas adaptativas de control de acceso— para mejorar, a la vez, la privacidad, la seguridad y la soberanía digital.

1.2. Justificación

a) Relevancia Científica

Vista desde lo epistemológico, esta tesis se pregunta cómo se construye, se valida y se legitima la identidad digital en sistemas descentralizados. La verificación de identidad se delegaba tradicionalmente a una autoridad central, pero las pruebas de conocimiento cero cambian esa lógica: permiten demostrar que algo es cierto sin revelar los datos personales de fondo (Zhou et al., 2020). Eso redefine lo que entendemos por conocimiento verificable y amplía la teoría de la confianza digital en entornos distribuidos.

b) Relevancia Tecnológica

La propuesta junta varias tecnologías disruptivas para resolver limitaciones que hoy son bastante concretas:

- Blockchain y credenciales verificables para garantizar trazabilidad e interoperabilidad.
- pruebas de conocimiento cero para autenticación y autorización selectiva.
- Cifrado homomórfico para procesar datos cifrados sin comprometer la privacidad.
- Control de acceso dinámico basado en atributos (ABAC) para gestionar permisos de forma adaptativa.

c) Relevancia Social y Normativa

En una sociedad tan conectada como la actual, gestionar la identidad digital de forma ética ya no es opcional. Por eso el modelo propuesto:

- Devuelve al usuario el control de sus credenciales.
- Fortalece la confianza digital en transacciones.
- Se alinea con normativas globales como RGPD y eIDAS 2.0.
- Promueve la protección de datos personales y la minimización de riesgos en entornos digitales.

1.3. Objetivo

1.3.1. Objetivo General

Evaluar comparativamente, mediante un diseño cuasi-experimental, un modelo avanzado de identidad digital descentralizada que integra blockchain, pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo, con el fin de determinar su impacto en la privacidad, la seguridad, la interoperabilidad, la usabilidad y la soberanía digital de los usuarios frente a modelos tradicionales y modelos de identidad autosoberana existentes.

1.3.2. Objetivos Específicos

- Analizar los riesgos de privacidad y seguridad en sistemas actuales de identidad digital descentralizada.
- Evaluar protocolos, estándares y marcos regulatorios relevantes: DID, VC, OAuth2, OpenID Connect, FIDO2, RGPD y eIDAS 2.0.
- Comparar el modelo propuesto con soluciones existentes, evaluando mejoras en seguridad, privacidad, interoperabilidad y usabilidad.

1.4. Hipótesis o Supuesto Hipotético

1.4.1. Hipótesis General

El modelo avanzado de identidad digital descentralizada que integra blockchain, pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo presenta mejoras significativas en privacidad, seguridad, interoperabilidad y soberanía digital, en comparación con los modelos centralizados tradicionales y las implementaciones básicas de identidad autosoberana.

1.5. Variables o Categoría de análisis

Tabla 1. Variables Independientes

Variable	Definición Operacional	Indicadores
Tecnología Blockchain	Implementación de un libro mayor distribuido para la gestión de credenciales verificables.	Consistencia, trazabilidad, latencia.
Zero-Knowledge Proofs	Uso de pruebas criptográficas para validar atributos sin exponer información sensible.	Reducción de datos expuestos.
Cifrado Homomórfico	Capacidad de realizar operaciones sobre datos cifrados sin necesidad de descifrarlos.	Nivel de confidencialidad mantenida.
Control de Acceso Adaptativo (ABAC)	Implementación de políticas dinámicas de permisos basadas en atributos y contexto.	Flexibilidad, granularidad de control.

Fuente: Elaboración propia.

Tabla 2. Variables Dependientes

Variable	Definición Operacional	Indicadores
Privacidad	Grado en que se limita la exposición de datos personales.	Volumen de datos revelados, cumplimiento RGPD.

Seguridad	Capacidad del sistema para prevenir accesos no autorizados.	Número de vulnerabilidades detectadas, ataques mitigados.
Soberanía Digital	Control que los usuarios tienen sobre sus credenciales.	Porcentaje de atributos gestionados localmente.
Usabilidad	Facilidad con que los usuarios interactúan con el sistema.	Tiempo medio de autenticación, tasa de éxito.
Interoperabilidad	Capacidad de integrarse con diferentes sistemas y proveedores.	Número de plataformas compatibles, adopción de estándares.

Fuente: Elaboración propia.

Tabla 3. Variables de Control

Variable de control	**Descripción / condición controlada**
Versión del protocolo DID/VC implementado	Se mantiene constante la versión del protocolo DID/VC utilizada durante las pruebas para garantizar comparabilidad entre los modelos evaluados.
Condiciones de red y capacidad de los servidores	Se controlan las condiciones de conectividad, latencia de red, capacidad de procesamiento, memoria y disponibilidad de los servidores utilizados en el entorno experimental.
Marcos regulatorios aplicados	Se consideran como referencia los marcos normativos RGPD y eIDAS 2.0 para evaluar el cumplimiento en términos de privacidad, minimización de datos, trazabilidad y control del usuario.
Tamaño y diversidad de la muestra de usuarios	Se controla la cantidad y características de los participantes o escenarios simulados para evitar sesgos y asegurar consistencia en la evaluación de usabilidad, privacidad y seguridad.

Fuente: Elaboración propia

2. Estado del arte, antecedentes y marco teórico-conceptual integrado

2.1. Estado del Arte

2.1.1. Criterios de construcción del estado del arte

El estado del arte se reorganiza a partir de una lógica analítica y no únicamente descriptiva. Para ello, se consideran aportes internacionales procedentes de estándares técnicos, literatura indexada y marcos regulatorios, así como aproximaciones latinoamericanas y nacionales asociadas a la protección de datos, confianza digital, identidad electrónica y servicios digitales. Esta perspectiva permite contrastar los desarrollos globales sobre DID, SSI, credenciales verificables y pruebas de conocimiento cero con las condiciones de adopción, gobernanza e interoperabilidad requeridas en contextos regionales.

La selección de fuentes se orienta por cuatro criterios: actualidad, pertinencia directa con identidad digital descentralizada, aporte metodológico o técnico verificable y relación con las variables de la investigación. En consecuencia, cada antecedente se analiza según su contribución a la privacidad, seguridad, interoperabilidad, usabilidad, soberanía digital o cumplimiento normativo, evitando que las investigaciones recientes queden aisladas del marco general del estado del arte.

Tabla 4. Criterios de construcción del estado del arte

Criterio	Aplicación en la revisión	Indicador documental	Relación con la tesis
Actualidad	Prioriza aportes recientes sin excluir bases teóricas fundacionales.	Año de publicación, vigencia del estándar o regulación.	Identifica avances 2020-2025 y conserva continuidad teórica.
Pertinencia temática	Selecciona documentos sobre DID, SSI, VC, ZKP, cifrado, ABAC/PBAC y privacidad.	Coincidencia con variables y dimensiones del estudio.	Asegura que el estado del arte responda al problema de investigación.
Rigor metodológico	Considera revisiones, estudios comparativos, pruebas empíricas,	Tipo de estudio, fuente, trazabilidad y calidad técnica.	Evita una revisión meramente narrativa y fortalece la base comparativa.

	estándares y marcos regulatorios.		
Perspectiva nacional e internacional	Contrasta desarrollos globales con exigencias regionales de protección de datos y confianza digital.	Contexto geográfico, marco legal y alcance de adopción.	Justifica la aplicabilidad del modelo en escenarios reales de gobernanza digital.

Fuente: Elaboración propia

La identidad digital se ha convertido en un componente esencial de la sociedad contemporánea, donde gran parte de las interacciones económicas, sociales, políticas y culturales se desarrollan en entornos digitales. En este contexto, garantizar la autenticidad de las identidades y la protección de los datos personales constituye un desafío técnico, ético y legal de primer orden. Tradicionalmente, la gestión de identidades digitales ha estado dominada por modelos centralizados, en los que una autoridad o proveedor concentra el control de las credenciales. Este enfoque, si bien facilitó la masificación de los servicios en línea, generó riesgos significativos de seguridad y privacidad, al exponer los datos de los usuarios a brechas, abusos y a la pérdida de soberanía sobre su propia información (Mühle et al., 2018).

La transición hacia modelos federados, con el uso de protocolos como SAML, OAuth2 y OpenID Connect, introdujo avances en interoperabilidad y experiencia de usuario, pero sin resolver la dependencia de un tercero de confianza. Dichos esquemas mantuvieron la asimetría de poder entre proveedores y usuarios, lo que abrió debates sobre la concentración de datos y la vulnerabilidad a prácticas de vigilancia masiva (Reece et al., 2022).

En respuesta a estas limitaciones, surge el paradigma de la identidad digital descentralizada (DID) y la identidad auto-soberana (identidad autosoberana, SSI), impulsado por las capacidades de blockchain y de credenciales verificables (Verifiable Credentials, VC) propuestas por el W3C. Bajo este modelo, los individuos tienen control directo sobre sus

credenciales, lo que reduce la dependencia de autoridades centralizadas y fortalece la privacidad y la soberanía digital (Goodell & Aste, 2019). Complementariamente, avances en pruebas de conocimiento cero (ZKP) y cifrado homomórfico ofrecen soluciones innovadoras para validar atributos o ejecutar operaciones sobre datos sin necesidad de exponer información sensible (Zhou et al., 2020; Schanzenbach et al., 2019).

Este nuevo enfoque de la identidad digital plantea oportunidades y desafíos. Entre las oportunidades se destacan el mayor control de los usuarios, la reducción de riesgos de fuga de datos y el cumplimiento más robusto de normativas como el Reglamento General de Protección de Datos (RGPD) y el eIDAS 2.0 en la Unión Europea (European Commission, 2023). No obstante, persisten desafíos vinculados a la escalabilidad, la interoperabilidad entre plataformas, la adopción masiva y la consolidación de marcos regulatorios globales.

En el marco de una investigación doctoral, la revisión del estado del arte no solo permite describir estas tecnologías y sus avances, sino también analizar sus limitaciones, evaluar comparativamente las propuestas existentes y proponer modelos innovadores. Esto se alinea con los niveles superiores de la Taxonomía de Bloom revisada: analizar, evaluar y crear (Anderson & Krathwohl, 2001).

2.2. Síntesis crítica del estado del arte

La bibliografía revisada deja ver un recorrido bastante claro: la identidad digital pasó de depender de una sola autoridad a modelos federados que reparten esa dependencia entre varios proveedores, y de ahí a los enfoques descentralizados que hoy giran en torno a DID, credenciales verificables y la llamada identidad autosoberana. Ese recorrido, sin embargo, no ha cerrado los problemas de fondo: privacidad, seguridad, interoperabilidad, usabilidad y cumplimiento

normativo siguen siendo puntos abiertos, y conviene no perderlos de vista al construir cualquier propuesta nueva.

Este panorama cambia bastante según desde dónde se mire. En Europa, el RGPD y el eIDAS 2.0 han armado un marco relativamente maduro, pensado para que las credenciales funcionen más allá de las fronteras de un solo país y para sostener la European Digital Identity Wallet (European Commission, 2023). Estados Unidos, en cambio, ha optado por guías técnicas sobre niveles de garantía de identidad más que por un reglamento único (NIST, 2020). En Ecuador el punto de partida es distinto: la Ley Orgánica de Protección de Datos Personales, vigente desde 2021, ya recoge principios como minimización, consentimiento y responsabilidad proactiva —tomados en buena medida del modelo europeo—, pero todavía no dice nada específico sobre identificadores descentralizados o credenciales verificables (Ecuador, Asamblea Nacional, 2021). Esa diferencia entre regiones no es un detalle menor: en América Latina el reto no es solo técnico, sino también normativo, porque los marcos legales apenas empiezan a nombrar blockchain, DID o VC de manera explícita, lo que refuerza la conveniencia de evaluar el modelo propuesto frente a más de un contexto regulatorio.

Volviendo a los modelos en sí: los centralizados funcionan bien y son fáciles de implementar, pero concentran datos personales, dependen de terceros y quedan expuestos ante cualquier brecha de seguridad. Los federados mejoran algo la experiencia del usuario y reducen la cantidad de credenciales que hay que manejar, aunque siguen atados a un proveedor de identidad y no le devuelven al usuario un control real sobre sus datos. Los descentralizados y autosoberanos sí representan un salto, porque el titular pasa a tener más control sobre la información; aun así, arrastran problemas propios, como la correlación de metadatos, la reutilización de identificadores, la escalabilidad de los procesos de revocación, una

interoperabilidad todavía limitada entre plataformas y una alineación imperfecta con marcos como el RGPD y el eIDAS 2.0.

A esto se suma que técnicas como las pruebas de conocimiento cero, el cifrado homomórfico o la divulgación selectiva sí logran reducir cuántos atributos terminan expuestos, pero casi siempre se estudian por separado. Es difícil encontrar una arquitectura que las junte todas —privacidad criptográfica, control de acceso adaptativo, trazabilidad verificable, interoperabilidad técnica y cumplimiento normativo— en un mismo diseño. Esa fragmentación es, en el fondo, el problema central: los sistemas de identidad digital necesitan soluciones que equilibren protección de datos, desempeño, experiencia de uso y validez jurídica a la vez, y no por partes.

De ahí surge la brecha que esta investigación intenta cerrar: no se encontró, en la revisión realizada, un modelo evaluado empíricamente que combine blockchain como ancla de confianza, pruebas de conocimiento cero para la divulgación selectiva, cifrado homomórfico para procesar atributos de forma segura y control de acceso adaptativo para decidir accesos según el contexto. Esa carencia es la que justifica el modelo que se propone en esta tesis, cuyo propósito es precisamente comprobar, de forma comparativa, si esa integración mejora la privacidad, la seguridad, la interoperabilidad, la usabilidad y la soberanía digital frente a los modelos centralizados tradicionales y frente a las implementaciones básicas de identidad autosoberana.

2.3. Evolución Histórica de la Identidad Digital

La gestión de la identidad digital no es un fenómeno reciente, sino el resultado de una evolución progresiva que acompaña el propio desarrollo de la web como espacio de interacción social y económica (Berners-Lee, 2000), y que responde a las demandas de seguridad,

interoperabilidad y soberanía del usuario en la era digital. Esta evolución puede dividirse en tres grandes etapas: centralizada, federada y descentralizada.

En la primera etapa, la identidad digital estuvo gestionada por autoridades centralizadas —generalmente gobiernos, bancos o grandes corporaciones— que almacenaban y controlaban las credenciales de los usuarios. Este enfoque garantizaba simplicidad administrativa, pero al mismo tiempo generaba un alto riesgo de concentración de datos. Una brecha de seguridad en un sistema centralizado podía comprometer millones de identidades simultáneamente. Ejemplos de este modelo incluyen los primeros sistemas de autenticación gubernamentales y corporativos, como Microsoft Passport en los años noventa, que buscaba unificar las credenciales de acceso a distintos servicios pero fracasó debido a la falta de confianza pública y a las críticas por exceso de centralización (Reece et al., 2022). Cabe señalar que, incluso antes de la consolidación de estos modelos centralizados, ya existían propuestas criptográficas orientadas a permitir transacciones sin identificación directa del usuario, las cuales anticiparon buena parte de los principios que hoy sustentan la identidad autosoberana (Chaum, 1985, 1992).

Este modelo centralizado demostró ser vulnerable no solo a ataques informáticos, sino también a prácticas de vigilancia y control excesivo, que reducían la autonomía del usuario y lo convertían en un sujeto pasivo de la gestión de su propia identidad (Mühle et al., 2018).

2.3.1. Identidad Federada

En una segunda etapa, surgió el modelo de identidad federada, cuyo objetivo fue reducir la fragmentación y mejorar la experiencia del usuario al permitir el uso de una misma credencial en diferentes servicios. Este esquema fue impulsado por alianzas y consorcios tecnológicos, como Liberty Alliance en los años 2000, que buscaba establecer un estándar abierto de autenticación entre múltiples proveedores, así como por principios rectores como las leyes de la

identidad, que buscaban orientar el diseño de sistemas de identidad centrados en el usuario (Cameron, 2005).

Más adelante, se consolidaron protocolos como OpenID y OAuth2, que permitieron a los usuarios acceder a diferentes plataformas utilizando las credenciales de un único proveedor de confianza (por ejemplo, iniciar sesión en un servicio con la cuenta de Google o Facebook). Estos avances redujeron la necesidad de múltiples contraseñas y facilitaron la interoperabilidad (Hardt, 2012).

Sin embargo, la federación mantuvo una dependencia estructural de terceros proveedores (los llamados identity providers), lo que concentró el poder en manos de unas pocas empresas tecnológicas y expuso a los usuarios a prácticas de explotación de datos, publicidad dirigida y riesgos de vigilancia masiva (Reece et al., 2022).

2.3.2. Identidad Descentralizada

La tercera y más reciente etapa corresponde al paradigma de la identidad digital descentralizada (DID) y la identidad auto-soberana (identidad autosoberana, SSI). Este modelo emergió en 2016, cuando se articuló formalmente la noción de identidad autosoberana como principio de diseño (Allen, 2016), con el impulso de la Fundación Sovrin y la publicación de las especificaciones de DID y Verifiable Credentials (VC) por parte del World Wide Web Consortium (W3C).

A diferencia de los modelos anteriores, la identidad descentralizada no depende de una autoridad central ni de un proveedor único, sino que se basa en tecnologías distribuidas como blockchain. Cada individuo puede crear, gestionar y compartir sus credenciales digitales de manera autónoma, sin necesidad de intermediarios. Además, las pruebas de conocimiento cero (ZKP) permiten demostrar atributos (como la mayoría de edad o el lugar de residencia) sin

revelar datos adicionales, mientras que el cifrado homomórfico habilita operaciones sobre datos cifrados (Zhou et al., 2020).

Este nuevo paradigma busca dar respuesta a los principios de privacidad por diseño, minimización de datos y soberanía digital, en consonancia con regulaciones internacionales como el RGPD y el eIDAS 2.0, que promueven un marco confiable para la gestión de la identidad digital en Europa (European Commission, 2023).

2.3.3. Síntesis de la evolución

La evolución histórica de la identidad digital demuestra una tendencia progresiva hacia la descentralización y el empoderamiento del usuario. Si los modelos centralizados y federados ofrecieron soluciones prácticas pero limitadas en términos de privacidad y control, la identidad descentralizada representa un avance hacia un modelo en el que los usuarios recuperan la soberanía sobre sus datos y se promueve un ecosistema más transparente y seguro.

En el marco de la investigación doctoral, este recorrido histórico permite analizar críticamente las limitaciones de los modelos pasados, evaluar comparativamente los logros de los esquemas descentralizados y crear propuestas innovadoras que integren blockchain, ZKP y cifrado homomórfico, alineadas con la Taxonomía de Bloom revisada (Anderson & Krathwohl, 2001).

2.4. Protocolos y Tecnologías Fundamentales en Identidad Digital Descentralizada

La arquitectura de la identidad digital descentralizada (DID) y de la identidad autosoberana (SSI) se sustenta en un conjunto de tecnologías y protocolos que garantizan la autenticación, la autorización, la integridad de los datos y el control de acceso. Estas herramientas no solo habilitan la gestión distribuida de las credenciales, sino que también ofrecen mecanismos de protección frente a amenazas emergentes en el ecosistema digital. Gran

parte de estos mecanismos criptográficos se apoya, en última instancia, en los fundamentos matemáticos de la criptografía de clave pública, formalizados por primera vez en los trabajos sobre intercambio de claves sin canal seguro previo (Diffie & Hellman, 1976) y sobre firmas digitales verificables mediante pares de claves pública y privada (Rivest et al., 1978). Estos principios, ampliamente documentados en la literatura de referencia sobre criptografía aplicada (Schneier, 2015), continúan siendo la base operativa de la firma de credenciales verificables y del anclaje criptográfico en blockchain.

2.4.1. Blockchain

La tecnología blockchain constituye la columna vertebral de la identidad digital descentralizada. Concebida originalmente como un libro mayor distribuido para sistemas de efectivo electrónico entre pares (Nakamoto, 2008), blockchain funciona como un registro distribuido, inmutable y transparente que permite almacenar anclajes criptográficos de credenciales verificables sin necesidad de un tercero central de confianza, apoyándose en funciones hash criptográficas cuya resistencia a colisiones garantiza la integridad de dichos anclajes (Preneel, 2010). Existen diferentes tipos de blockchain aplicadas a la identidad:

- Públicas (como Ethereum): abiertas y descentralizadas, aunque con limitaciones de escalabilidad y privacidad (Buterin, 2014; Wood, 2014).
- Privadas: controladas por una organización, con mayor eficiencia, pero menor descentralización.

Permisionadas (como Hyperledger Indy): buscan un equilibrio entre descentralización y gobernanza controlada (Goodell & Aste, 2019).

El uso de blockchain en identidad ofrece trazabilidad y resistencia a manipulaciones, pero también plantea retos como el almacenamiento permanente de metadatos y los costos de

transacción (Zhou et al., 2020), aspectos ampliamente documentados en revisiones sistemáticas sobre los desafíos de seguridad de blockchain (Guo & Yu, 2022). Este potencial se apoya en el concepto de contratos inteligentes, formalizado antes de la existencia de blockchains operativas como una forma de codificar acuerdos verificables sobre redes públicas (Szabo, 1997), así como en propuestas tempranas de dinero digital descentralizado que precedieron directamente al diseño de Bitcoin (Szabo, 2002), y se ha sistematizado posteriormente mediante taxonomías que clasifican las arquitecturas blockchain según su gobernanza, consenso y modelo de datos (Xu et al., 2017; Yaga et al., 2019). Estas clasificaciones técnicas, junto con panoramas integrales de las tecnologías de criptomonedas y libros de contabilidad distribuidos (Narayanan et al., 2016), permiten fundamentar por qué la identidad digital descentralizada recurre preferentemente a configuraciones permisionadas antes que a cadenas públicas sin control de acceso.

2.4.2. pruebas de conocimiento cero (ZKP)

Las pruebas de conocimiento cero (pruebas de conocimiento cero, ZKP) son un avance criptográfico que permite a un usuario demostrar la veracidad de una afirmación sin necesidad de revelar la información subyacente. Por ejemplo, un ciudadano puede probar que es mayor de edad sin revelar su fecha de nacimiento. Existen variantes como:

- ZK-SNARKs: pruebas breves y no interactivas, utilizadas en criptomonedas como Zcash mediante esquemas de credenciales anónimas descentralizadas (Garman et al., 2016; Zcash Foundation, 2019).
- ZK-STARKs: más escalables y sin necesidad de configuración inicial de confianza.
- Bulletproofs: pruebas más eficientes para rangos de valores (Schanzenbach et al., 2019).

El potencial de las ZKP en identidad digital radica en minimizar la exposición de datos sensibles y prevenir ataques de correlación. Estas pruebas encuentran su fundamento teórico en

los desarrollos formales de la criptografía moderna que establecieron las bases matemáticas de la demostración interactiva y no interactiva de conocimiento (Goldreich, 2001).

2.4.3. Cifrado Homomórfico

El cifrado homomórfico permite realizar cálculos sobre datos cifrados sin necesidad de descifrarlos previamente. Esto significa que una institución puede verificar la validez de una credencial sin tener acceso a la información sensible en claro. Junto con enfoques como la privacidad diferencial, que introduce ruido estadístico controlado para limitar la re-identificación de individuos en conjuntos de datos agregados (Dwork, 2006), el cifrado homomórfico amplía el repertorio de técnicas criptográficas orientadas a minimizar la exposición de atributos personales.

- Parcial: admite un número limitado de operaciones matemáticas (suma o multiplicación).
- Completo: permite realizar cualquier cálculo sobre datos cifrados, aunque todavía presenta altos costos computacionales (Zhou et al., 2020).

En el contexto de DID, el cifrado homomórfico se proyecta como un complemento crucial para sectores como la salud y las finanzas, donde los datos personales son altamente sensibles.

2.4.4. Protocolos de Autenticación y Autorización (OAuth2 y OpenID Connect)

Los protocolos OAuth2 y OpenID Connect constituyen estándares en la autenticación federada, y aunque provienen del paradigma centralizado, han sido adaptados para integrarse en soluciones de identidad descentralizada.

OAuth2 se centra en la autorización delegada, permitiendo que un usuario otorgue permisos limitados a una aplicación sin compartir sus credenciales completas (Hardt, 2012).

OpenID Connect, sobre OAuth2, añade una capa de autenticación, posibilitando a los usuarios iniciar sesión de forma segura en diferentes servicios con un mismo conjunto de credenciales.

Su integración en SSI busca facilitar la interoperabilidad con sistemas heredados, garantizando una transición más fluida hacia entornos descentralizados, en un proceso que converge con estándares de autenticación sin contraseñas orientados a fortalecer la resistencia al phishing (FIDO Alliance, 2022).

2.4.5. Modelos de Control de Acceso (RBAC, ABAC y PBAC)

El control de acceso es un componente clave en la seguridad de los sistemas de identidad, entendida no solo como un conjunto de mecanismos técnicos sino como una disciplina orientada a gestionar el riesgo real en entornos operativos (Lampson, 2004). Se destacan tres modelos principales:

- RBAC (Role-Based Access Control): basado en roles predefinidos; simple, pero rígido.
- ABAC (Attribute-Based Access Control): dinámico, concede permisos en función de atributos del usuario y el contexto (por ejemplo, ubicación, dispositivo o nivel de riesgo).
- PBAC (Policy-Based Access Control): establece reglas más amplias basadas en políticas de seguridad, combinando atributos y roles (Hu et al., 2015).

En entornos de identidad descentralizada, ABAC y PBAC se perfilan como los más adecuados al ofrecer un control granular y adaptativo.

2.5. Plataformas y Proyectos Relevantes en Identidad Digital Descentralizada

La transición hacia un modelo de identidad digital descentralizada (DID) no ha sido solo conceptual o normativa, sino también práctica, una tendencia documentada también en análisis de mercado sobre la adopción empresarial de tecnologías de identidad digital (Thibodeau, 2021).

Distintos proyectos y plataformas han materializado los principios de la identidad autosoberana (SSI) y ofrecen una base empírica para evaluar los avances y retos del campo. A continuación, se presentan los proyectos más influyentes: Hyperledger Indy, Sovrin, uPort, Civic, Microsoft Entra y SpruceID, todos ellos con aportes significativos en privacidad, seguridad, interoperabilidad y soberanía digital.

2.5.1. Hyperledger Indy

Hyperledger Indy, impulsado por la Linux Foundation, es una plataforma permisionada diseñada específicamente para la gestión de identidades digitales descentralizadas. Implementa nativamente identificadores descentralizados (DID), credenciales verificables (VC) y mecanismos de divulgación selectiva, lo que permite que los usuarios compartan únicamente los atributos estrictamente necesarios durante un proceso de verificación (Mühle et al., 2018). Su arquitectura está orientada a separar las funciones de emisión, almacenamiento, presentación y verificación de credenciales, favoreciendo un modelo en el que el titular conserva mayor control sobre sus datos personales y puede reducir la exposición innecesaria de información sensible.

Una de las principales fortalezas de Hyperledger Indy es su enfoque especializado en identidad autosoberana, a diferencia de otras plataformas blockchain de propósito general. Indy incorpora componentes diseñados para la emisión y verificación de credenciales, la resolución de identificadores descentralizados y la gestión de pruebas criptográficas asociadas a atributos verificables. Esto lo convierte en una referencia relevante dentro del ecosistema SSI, ya que permite analizar cómo una infraestructura distribuida puede ofrecer trazabilidad, integridad y verificabilidad sin requerir que los datos personales se almacenen directamente en la cadena.

Relevancia en la tesis: Indy representa un ejemplo sólido de cómo una arquitectura blockchain orientada a identidad puede proteger la privacidad y, al mismo tiempo, garantizar la

verificabilidad de las credenciales. Su uso de divulgación selectiva resulta especialmente pertinente para esta investigación, ya que se relaciona con el objetivo de minimizar la exposición de atributos personales y fortalecer la soberanía digital del usuario. No obstante, su carácter permisionado y su dependencia de una gobernanza específica también evidencian limitaciones importantes en términos de escalabilidad global, interoperabilidad con otros ecosistemas y adopción masiva. Por ello, Hyperledger Indy se considera en esta tesis como un punto de referencia técnico para comparar las ventajas y restricciones de las arquitecturas SSI existentes frente al modelo avanzado propuesto.

2.5.2. Sovrin

Sovrin se construyó sobre Hyperledger Indy y añadió un marco de gobernanza global conocido como Sovrin Governance Framework, cuyo propósito es establecer reglas, roles, responsabilidades y criterios de confianza para los distintos actores que participan en el ecosistema de identidad digital descentralizada (Tobin & Reed, 2016). A diferencia de una blockchain pública sin control institucional definido, Sovrin propone una red permisionada orientada a identidad autosoberana, en la que intervienen emisores, titulares, verificadores, administradores de nodos y entidades de gobernanza. Este enfoque busca combinar la verificabilidad criptográfica propia de las tecnologías distribuidas con un marco normativo y operativo que permita generar confianza entre organizaciones, usuarios y proveedores de servicios (Goodell & Aste, 2019), en línea con los planteamientos sobre gobernanza de blockchain que subrayan la necesidad de reglas explícitas de coordinación entre actores descentralizados (Berg et al., 2019).

Uno de los aportes más relevantes de Sovrin es que no limita la identidad descentralizada a un problema exclusivamente técnico. Su modelo reconoce que la confianza digital también

requiere reglas de participación, mecanismos de auditoría, responsabilidades institucionales y criterios de cumplimiento. En este sentido, la plataforma permite analizar cómo una arquitectura SSI puede articular componentes criptográficos, como DID y credenciales verificables, con principios de gobernanza que regulen la emisión, validación, revocación y uso de credenciales digitales. Esto resulta especialmente importante en contextos donde las credenciales tienen valor jurídico, financiero, académico o administrativo.

Desde una perspectiva de privacidad, Sovrin busca reducir la dependencia de proveedores centralizados de identidad, permitiendo que el usuario conserve mayor control sobre sus credenciales y decida qué atributos compartir en cada interacción. No obstante, su estructura permisionada y su modelo de gobernanza también plantean desafíos importantes. Entre ellos se encuentran la escalabilidad internacional, la interoperabilidad con otros ecosistemas DID/VC, la aceptación por parte de entidades públicas y privadas, y la necesidad de adecuarse a marcos regulatorios como RGPD y eIDAS 2.0, especialmente en lo relacionado con minimización de datos, consentimiento, portabilidad, revocación y reconocimiento transfronterizo de credenciales (European Commission, 2023).

Relevancia en la tesis: Sovrin es clave porque demuestra que la identidad digital descentralizada no puede depender únicamente de la seguridad criptográfica, sino que requiere una capa de gobernanza capaz de definir confianza, responsabilidad y cumplimiento normativo. Para esta investigación, Sovrin constituye un referente importante porque evidencia la necesidad de integrar seguridad técnica, protección jurídica y soberanía del usuario dentro de una misma arquitectura. Sin embargo, también permite identificar limitaciones que justifican el modelo propuesto, especialmente la necesidad de fortalecer la privacidad mediante pruebas de

conocimiento cero, reducir riesgos de correlación, mejorar la interoperabilidad y complementar la gobernanza con mecanismos adaptativos de control de acceso y cumplimiento normativo.

2.5.3. uPort / Veramo

uPort fue uno de los primeros proyectos en desplegar identificadores descentralizados sobre la red Ethereum, permitiendo que los usuarios gestionaran directamente sus credenciales digitales en un entorno Web3. Su propuesta inicial se orientó a otorgar mayor autonomía al titular de la identidad mediante el uso de billeteras digitales, contratos inteligentes y mecanismos de verificación descentralizada. A través de este enfoque, uPort buscó reducir la dependencia de proveedores centralizados de identidad y promover un modelo en el que el usuario pudiera controlar sus datos, autorizar interacciones y presentar credenciales verificables en distintos servicios digitales (Reece et al., 2022).

Con el tiempo, uPort evolucionó hacia Veramo, un framework modular y extensible para la creación, resolución, administración y verificación de identificadores descentralizados y credenciales verificables. Veramo amplía la visión original de uPort al ofrecer una arquitectura más flexible, compatible con múltiples métodos DID, distintos formatos de credenciales y diversos entornos de implementación. Esta evolución refleja una tendencia importante en el ecosistema de identidad descentralizada: pasar de soluciones específicas basadas en una blockchain determinada hacia marcos interoperables capaces de adaptarse a diferentes infraestructuras, casos de uso y necesidades organizacionales.

Desde la perspectiva de la soberanía digital, uPort/Veramo representa un caso relevante porque demuestra que es posible trasladar el control operativo de la identidad hacia el usuario, permitiendo que este gestione sus credenciales desde una billetera y decida cuándo y cómo compartirlas. Sin embargo, el uso de cadenas públicas como Ethereum también revela desafíos

importantes. La transparencia de las redes públicas puede facilitar la exposición de metadatos, la correlación entre transacciones y la reconstrucción de patrones de comportamiento, especialmente cuando se reutilizan identificadores o se generan interacciones frecuentes con contratos inteligentes. Por tanto, aunque este tipo de soluciones fortalece la autonomía del usuario, también puede introducir nuevos riesgos de privacidad si no se incorporan mecanismos adicionales de protección.

Relevancia en la tesis: uPort/Veramo evidencia el potencial de la identidad digital descentralizada en entornos Web3, especialmente en lo relacionado con control del usuario, portabilidad de credenciales e interoperabilidad entre servicios. No obstante, también muestra una de las tensiones centrales que aborda esta investigación: la descentralización no garantiza por sí sola privacidad. La exposición de metadatos en cadenas públicas, la posibilidad de correlación entre interacciones y la persistencia de registros verificables justifican la necesidad de incorporar mecanismos criptográficos avanzados. En este sentido, las pruebas de conocimiento cero, el cifrado homomórfico y las políticas de control de acceso adaptativo propuestas en esta tesis actúan como mecanismos complementarios para reducir la exposición de información sensible, fortalecer la no vinculabilidad y mantener la soberanía digital sin sacrificar verificabilidad ni trazabilidad.

2.5.4. Civic

Civic se centra en la verificación de identidad y en procesos reutilizables de conocimiento del cliente y prevención de lavado de activos (KYC/AML), especialmente en el sector financiero, servicios digitales regulados y aplicaciones basadas en blockchain. Su propuesta consiste en permitir que el usuario verifique determinados atributos de identidad una sola vez y posteriormente pueda reutilizarlos en distintos servicios, reduciendo la repetición de

procesos de validación y la exposición innecesaria de documentos personales. Para ello, Civic utiliza mecanismos de anclaje en blockchain que permiten verificar la integridad y trazabilidad de las credenciales, mientras que los datos sensibles permanecen bajo control del usuario o fuera de la cadena, evitando su almacenamiento directo en registros públicos o sistemas centralizados de alto riesgo (Goodell & Aste, 2019).

Desde el punto de vista de privacidad, Civic aporta un enfoque pragmático basado en la minimización de datos. En lugar de solicitar repetidamente información completa del usuario, el modelo permite validar atributos específicos requeridos por un proveedor de servicio, como identidad verificada, mayoría de edad o cumplimiento de requisitos KYC, sin necesidad de compartir todos los datos personales en cada interacción. Esta lógica se alinea con los principios de privacidad por diseño y minimización establecidos en marcos regulatorios como el RGPD, ya que busca limitar la información divulgada a lo estrictamente necesario para una finalidad concreta.

Asimismo, Civic resulta relevante porque muestra una aplicación práctica de la identidad digital descentralizada en sectores donde la confianza, la trazabilidad y el cumplimiento normativo son requisitos críticos. En el ámbito financiero, por ejemplo, los procesos KYC/AML suelen implicar la recopilación repetida de documentos sensibles por múltiples instituciones, lo que incrementa riesgos de exposición, duplicidad y brechas de seguridad. Un esquema reutilizable de verificación permite reducir estas fricciones, mejorar la experiencia del usuario y disminuir la superficie de ataque asociada al almacenamiento disperso de datos personales.

No obstante, Civic también presenta limitaciones importantes desde la perspectiva de la identidad autosoberana plena. Aunque promueve la minimización y la reutilización de verificaciones, su funcionamiento puede mantener dependencia de emisores, validadores o

proveedores de confianza que certifican inicialmente la identidad del usuario. Esta dependencia introduce una tensión entre eficiencia operativa y soberanía digital, ya que el usuario conserva mayor control sobre el uso de sus credenciales, pero no necesariamente controla por completo el proceso de emisión, validación o revocación. Además, al operar en contextos regulados, el modelo debe equilibrar privacidad con obligaciones de auditoría, trazabilidad y cumplimiento legal.

Relevancia en la tesis: Civic aporta un referente útil para comprender cómo los modelos de identidad descentralizada pueden aplicarse a escenarios reales de verificación reutilizable y cumplimiento KYC/AML, manteniendo una orientación hacia la minimización de datos. Sin embargo, también evidencia que la reducción de exposición de información no es suficiente para alcanzar una identidad autosoberana robusta si persisten dependencias de emisores centralizados o mecanismos limitados de no vinculabilidad. Por ello, esta tesis toma a Civic como un caso de referencia para justificar la necesidad de un modelo avanzado que complemente la minimización de datos con pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo, permitiendo fortalecer la privacidad, reducir riesgos de correlación y mejorar la soberanía digital del usuario en entornos regulados.

2.5.5. Microsoft Entra (Verified ID)

Microsoft Entra Verified ID, anteriormente conocido como Azure Active Directory Verifiable Credentials, constituye una solución orientada a la emisión, administración y verificación de credenciales digitales dentro del ecosistema empresarial de Microsoft. Esta plataforma permite integrar credenciales verificables con servicios corporativos como Azure, Microsoft 365 y sistemas de gestión de identidad organizacional, siguiendo los principios de los estándares W3C DID/VC. Su enfoque está dirigido principalmente a instituciones, empresas y

organizaciones que requieren mecanismos confiables de autenticación, validación de atributos y gestión de accesos en entornos digitales complejos (Reece et al., 2022). Microsoft Entra Verified ID implementa el modelo de identidad descentralizada documentado en las especificaciones técnicas de la compañía sobre identificadores descentralizados y credenciales verificables (Microsoft, 2021).

A diferencia de proyectos más orientados a la descentralización abierta, Microsoft Entra Verified ID se ubica en un contexto empresarial donde la identidad digital debe integrarse con directorios corporativos, políticas internas de seguridad, flujos de cumplimiento normativo y mecanismos de administración centralizada. Esto permite facilitar la adopción de credenciales verificables en organizaciones que ya utilizan infraestructuras Microsoft, reduciendo la complejidad de implementación y favoreciendo la interoperabilidad con servicios existentes. En este sentido, la plataforma demuestra que los modelos DID/VC pueden incorporarse progresivamente en sistemas corporativos sin reemplazar por completo las arquitecturas de identidad tradicionales.

Desde la perspectiva de seguridad, Microsoft Entra Verified ID aporta ventajas relevantes para la verificación de atributos laborales, certificaciones, permisos de acceso, identidad de empleados, validación de proveedores y control de credenciales organizacionales. La posibilidad de emitir credenciales verificables permite disminuir la dependencia de documentos físicos o verificaciones manuales, al tiempo que fortalece la trazabilidad y confiabilidad de los procesos de autenticación. Sin embargo, al operar dentro de un ecosistema empresarial administrado, el grado de soberanía del usuario puede verse condicionado por políticas organizacionales, controles corporativos y decisiones centralizadas sobre emisión, revocación y acceso a credenciales.

Relevancia en la tesis: Microsoft Entra Verified ID muestra cómo los principios de identidad autosoberana y credenciales verificables pueden adaptarse a contextos corporativos reales, donde la interoperabilidad, la facilidad de adopción y la integración con sistemas heredados son factores determinantes. Para esta investigación, constituye un referente importante porque evidencia la posibilidad de aplicar estándares DID/VC en ambientes empresariales, pero también permite identificar una tensión central: el equilibrio entre usabilidad corporativa, gobernanza institucional y soberanía digital del usuario. Esta tensión justifica la necesidad de un modelo avanzado que combine interoperabilidad empresarial, privacidad criptográfica, control de acceso adaptativo y mecanismos de minimización de datos, evitando que la identidad descentralizada quede limitada por lógicas excesivamente centralizadas o dependientes de un único proveedor tecnológico.

2.5.6. SpruceID

SpruceID destaca por su orientación hacia la interoperabilidad multi-blockchain, la portabilidad de credenciales digitales y la construcción de soluciones de identidad descentralizada compatibles con distintos ecosistemas tecnológicos. Su propuesta se enfoca en permitir que los usuarios puedan emitir, almacenar, presentar y verificar credenciales digitales en diferentes entornos, evitando la dependencia de una única red, plataforma o proveedor. Esta característica resulta especialmente relevante en el ámbito de la identidad autosoberana, donde la portabilidad y el control del usuario sobre sus datos constituyen principios fundamentales para reducir la concentración de información y fortalecer la soberanía digital (Zhou et al., 2020).

Una de las principales fortalezas de SpruceID es su enfoque orientado a estándares abiertos y a la integración con tecnologías emergentes del ecosistema Web3. Al facilitar la interacción entre credenciales verificables, identificadores descentralizados y diferentes

infraestructuras blockchain, SpruceID permite analizar cómo una arquitectura de identidad puede mantenerse flexible, portable e interoperable en contextos heterogéneos. Esto resulta importante porque uno de los principales retos de los modelos DID/VC es evitar la fragmentación tecnológica, es decir, que las credenciales emitidas en una plataforma no puedan ser verificadas o reutilizadas en otra.

Desde la perspectiva de privacidad, SpruceID contribuye a fortalecer el control del titular sobre sus credenciales, al permitir que los datos personales no dependan exclusivamente de repositorios centralizados. Asimismo, su orientación hacia la portabilidad favorece que el usuario pueda utilizar sus credenciales en distintos servicios digitales sin necesidad de repetir procesos de registro, validación o entrega excesiva de información personal. Sin embargo, su aplicación también enfrenta desafíos vinculados con la escalabilidad, la gobernanza entre múltiples redes, la compatibilidad entre estándares y la protección frente a riesgos de correlación cuando una misma identidad interactúa en diferentes ecosistemas.

Relevancia en la tesis: SpruceID constituye un referente importante porque evidencia la necesidad de construir modelos de identidad digital descentralizada que sean escalables, portables e interoperables. Su enfoque se alinea con la hipótesis doctoral de esta investigación, orientada a evaluar una solución avanzada capaz de maximizar la privacidad, la seguridad, la interoperabilidad y la soberanía digital del usuario. No obstante, también permite identificar una brecha relevante: la interoperabilidad por sí sola no garantiza privacidad ni reducción de riesgos de correlación. Por ello, el modelo propuesto en esta tesis busca complementar esa visión mediante la integración de pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo, con el fin de ofrecer una arquitectura más robusta, verificable y alineada con principios de minimización de datos.

2.6. Retos y limitaciones en la identidad digital descentralizada

La evolución hacia SSI/DID ha mostrado avances sustantivos en control del usuario y verificabilidad criptográfica; sin embargo, persisten cuatro frentes críticos que condicionan su adopción a gran escala: (i) escalabilidad, (ii) interoperabilidad, (iii) ataques de correlación y riesgos de metadatos, y (iv) cumplimiento normativo (RGPD y eIDAS 2.0). A continuación, se examina cada uno con enfoque analítico y propuestas técnicas y metodológicas alineadas con los objetivos de tu tesis.

2.6.1. Escalabilidad

Problema. Los flujos SSI combinan operaciones on-chain (anclaje de schemas, definiciones de credenciales, métodos DID y, en algunos casos, listas de revocación) con verificación off-chain (presentaciones, pruebas criptográficas). La escalabilidad se ve afectada por: (a) límite de rendimiento de ledgers públicos/permisionados, (b) latencias en resolución de DIDs y revocación, y (c) coste computacional de pruebas avanzadas (p. ej., ZK-SNARKs/STARKs) (Goodell & Aste, 2019; Zhou et al., 2020). Esta limitación coincide con los hallazgos generales sobre la dificultad de escalar arquitecturas de registro distribuido sin sacrificar descentralización o seguridad (Vukolić, 2016). En soluciones basadas en credenciales con divulgación selectiva (p. ej., AnonCreds), el seguimiento y distribución de evidencias de revocación puede convertirse en cuello de botella en ecosistemas con millones de titulares (Mühle et al., 2018).

Mitigación técnica.

- Arquitecturas híbridas: anclar solo hashes y schemas en cadena; mantener credenciales y status lists comprimidos off-chain con pruebas verificables (Goodell & Aste, 2019).
- Acumuladores criptográficos y listas de estado compactas para revocación a gran escala.

- ZKP más eficientes (p. ej., BBS+/Bulletproofs) para reducir tamaño/tiempo de verificación (Schanzenbach et al., 2019).
- Métricas recomendadas (para la evaluación doctoral): TPS efectivo de emisión/verificación, latencia P95 de presentación, costo de verificación por prueba, tiempo medio de propagación de revocación, y porcentaje de verificaciones offline exitosas (Zhou et al., 2020).

2.6.2. Interoperabilidad

Problema. La interoperabilidad implica al menos tres planos: (a) métodos DID (p. ej., did:indy, did:ethr, did:key), (b) formatos de credenciales y presentaciones (JSON-LD/LD-Proofs vs JWT-VC), y (c) protocolos de intercambio (agentes Aries/mediación, OIDC4VCI/OIDC4VP). La coexistencia de variantes y capas provoca fragmentación semántica y dependencia de ecosistemas específicos (Reece et al., 2022). Además, la integración con sistemas heredados (SAML, OAuth2/OIDC corporativo) sigue siendo un reto práctico.

Mitigación técnica.

- Puentes y perfiles de interoperabilidad (conjuntos mínimos de requisitos) entre formatos VC-JWT y VC-LD, y resolutores DID multi-método (Reece et al., 2022).
- Normalización de claims y ontologías (mapeos de atributos) para evitar ambigüedad semántica.
- Compatibilidad gradual con OIDC/SAML (p. ej., OIDC4VCI para emisión, OIDC4VP para presentación) como estrategia de transición.
- Métricas recomendadas: tasa de verificación cruzada entre wallets/verifiers heterogéneos, tiempo de resolución DID multi-método, y porcentaje de fallos por desalineación semántica de atributos (Mühle et al., 2018; Reece et al., 2022).

2.6.3. Ataques de correlación y riesgos de metadatos

Problema. Aunque la credencial no se publique en la cadena, metadatos derivados (reutilización de DIDs, timing, IP, user agent, verifier collusion) permiten correlacionar presentaciones de un mismo titular entre dominios, erosionando el unlinkability. Además, la transparencia de ciertos ledgers facilita análisis indirectos (Zhou et al., 2020), en línea con estudios empíricos que demostraron que el análisis de patrones de transacciones en registros públicos permite des-anonimizar a participantes incluso sin acceso a datos personales explícitos (Meiklejohn et al., 2013). El empleo de credenciales con atributos estáticos sin blinding o sin divulgación selectiva potencia la re-identificación (Mühle et al., 2018).

Mitigación técnica.

- DIDs pareados (pairwise) y rotación de identificadores por relación/verificación.
- Firmas BBS+ y ZKP para divulgación selectiva y no-vinculabilidad entre sesiones (Schanzenbach et al., 2019).
- Canales con privacidad (mediación, relays, blinding de endpoints) y minimización de logs en verificadores.
- Políticas de minimización: exponer solo atributos estrictamente necesarios; evitar timestamps de alta resolución.

Métricas recomendadas: índice de vinculabilidad entre presentaciones, entropía de identificadores pareados, y reducción del volumen de datos revelados por transacción (Zhou et al., 2020).

2.6.4. Cumplimiento normativo (RGPD y eIDAS 2.0)

Problema. La SSI debe alinearse con principios de privacidad (licitud, lealtad, transparencia, minimización, limitación de finalidad) y con derechos como acceso, portabilidad y

supresión (RGPD). La inmutabilidad de blockchain choca con el derecho al olvido, mientras que la ambigüedad de roles (¿quién es controller y quién processor?) complica la asignación de responsabilidades. Con eIDAS 2.0, la European Digital Identity Wallet exige garantías técnicas y de gobernanza adicionales, así como reconocimiento transfronterizo de credenciales de "alto nivel de garantía" (European Commission, 2023). El ISO/IEC 29100 aporta un marco de privacidad aplicable, pero no resuelve por sí solo las tensiones entre inmutabilidad y supresión (ISO/IEC, 2011).

Mitigación técnica y de gobernanza.

- Anclajes off-chain: almacenar datos personales fuera de la cadena; en cadena solo referencias criptográficas revocables.
- Revocación y expiración como mecanismos funcionales de "olvido" (desvinculación práctica del dato).
- Modelos de gobernanza (tipo Sovrin) que clarifiquen roles, responsabilidades y auditoría (Goodell & Aste, 2019).
- Evaluaciones de impacto de privacidad (DPIA) y modelos de riesgo por contexto de uso.
- Métricas recomendadas: grado de minimización de datos por flujo, tiempo de atención a derechos (acceso/rectificación/supresión), y alineación de controles con eIDAS 2.0 (European Commission, 2023; ISO/IEC, 2011).

2.7. Investigaciones recientes vinculadas al estado del arte

Este apartado se integra al estado del arte mediante una lectura crítica de las investigaciones recientes y no como un listado separado de publicaciones. Los aportes se organizan según la brecha que atienden: interoperabilidad, divulgación selectiva, reducción de datos, seguridad,

gobernanza y cumplimiento normativo. Esta vinculación permite comprender cómo cada avance reciente contribuye o limita la construcción del modelo propuesto.

Desde una postura internacional, la literatura evidencia una transición desde arquitecturas SSI generales hacia mecanismos específicos de privacidad verificable, como BBS+, SD-JWT VC, OIDC4VCI/OIDC4VP y pruebas de conocimiento cero. Desde una postura regional y nacional, el reto principal no se limita a la adopción técnica, sino a la compatibilidad con marcos de protección de datos, procesos de confianza digital, reconocimiento jurídico de credenciales y condiciones institucionales de interoperabilidad. Esta doble lectura permite ubicar la tesis en una discusión técnica y sociojurídica más amplia.

La investigación de 2024–2025 se ha concentrado en cinco ejes: (i) estandarización e interoperabilidad para issuance y presentations, (ii) mecanismos criptográficos de divulgación selectiva y no-vinculabilidad (BBS+, SD-JWT, ZKPs), (iii) evaluaciones de minimización de datos y revocación, (iv) estudios de seguridad model-driven y (v) aplicaciones verticales (salud, IoT, metrología), con un esfuerzo notable por alinear resultados con RGPD/eIDAS 2.0.

2.7.1. Estandarización e interoperabilidad (OIDC4VCI/OIDC4VP, BBS+)

Las especificaciones OpenID for Verifiable Credentials avanzaron con profiles para emisión (OIDC4VCI) y presentación (OIDC4VP), buscando compatibilidad con infraestructuras OIDC/SAML existentes y wallets heterogéneas; informes técnicos y notas de adopción en 2024 subrayan su papel como “puente” entre Web2 y SSI, y reportan casos de interoperabilidad premiados en EIC 2024 (lo que respalda su madurez pre-productiva). Paralelamente, el W3C consolidó el BBS+ Data Integrity Cryptosuite (2023→), que habilita divulgación selectiva y pruebas derivadas no vinculables sobre credenciales JSON-LD, clave para reducir correlación entre verificaciones. (MATTR, 2024; OpenID Foundation, 2024; W3C, 2023).

2.7.2. Divulgación selectiva y ZKPs: estado del arte y propuestas

En Elsevier (Bećirović Ramić et al., 2024) se publicaron revisiones sistemáticas de divulgación selectiva que clasifican enfoques (compromisos/SD-JWT, ZKPs tipo BBS+, Bulletproofs y STARKs) y discuten ventajas/desventajas operativas (tamaño de prueba, tiempos de verificación, compatibilidad con formatos JSON/JWT). Computer Standards & Interfaces (2024) amplía el análisis con el foco criptográfico comparado para VC, mientras arXiv (2024–2025) propone esquemas nuevos (p. ej., BLS-MT-ZKP, SD-BLS con revocación umbral no vinculable) que prometen reducir huella y acelerar revocación a gran escala. (Bećirović Ramić et al., 2024; Roio et al., 2024; Oneto et al., 2024).

2.7.3. Minimización de datos y medición empírica

Un trabajo Elsevier (Piskozub et al., 2025) evalúa empíricamente distintos tipos de credenciales (BBS+-JSON, AnonCreds, etc.) y concluye que los formatos JSON-VC con ZKP facilitan minimización de datos y presentaciones más ligeras frente a alternativas sin divulgación selectiva. Esta evidencia apoya el uso de BBS+/ZKP en escenarios de alto cumplimiento (p. ej., eIDAS 2.0), y sugiere métricas para comparar overhead y tamaño de prueba en presentaciones reales. (Piskozub et al., 2025).

2.7.4. Seguridad y análisis model-driven

Desde arXiv (2024) se propone un marco de análisis de seguridad model-driven para patrones arquitectónicos SSI, con verificación mediante model checking y catálogos de patrones vulnerables (p. ej., reutilización de DIDs, puntos únicos de correlación en mediación, revocación con leakage de metadatos). Esta línea es especialmente útil para tu tesis porque operacionaliza propiedades de seguridad (temporal lógicas) que pueden convertirse en métricas de evaluación. (Ding & Sato, 2024).

2.7.5. Aplicaciones verticales (salud, metrología/industria, IoT)

En Elsevier (FGCS/CEE, 2024–2025) se exploran SSI+DID en salud (Web3 healthcare con esquemas DID-HVC y divulgación selectiva) y en metrología (certificados de calibración digitales con presentaciones verificables que revelan solo metadatos requeridos). En paralelo, conferencias técnicas muestran SSI para IoT/WoT, analizando autenticación y gestión de credenciales en dispositivos restringidos. Estas pruebas de concepto confirman la viabilidad práctica y ayudan a acotar requisitos de desempeño para edge, un escenario que retoma preocupaciones tempranas sobre los riesgos de seguridad y privacidad introducidos por la proliferación de dispositivos conectados (Weber, 2010), y que converge con propuestas de gestión de identidad basada en blockchain orientadas a sectores con múltiples partes verificadoras (Sun et al., 2021). (Zhang et al., 2024; da Silva et al., 2025; Boi et al., 2024).

2.7.6. Encuestas y panoramas 2024–2025

El panorama más completo y reciente es la encuesta de DIDs/VCs (2024→2025) que cataloga implementaciones, dominios de aplicación, amenazas y regulaciones emergentes; el artículo (con DOI de arXiv y mención de referencia en IEEE Communications Surveys & Tutorials, 2025) se ha convertido en punto de referencia para delimitar tendencias y brechas del ecosistema. En paralelo, las encuestas de ZKP (2024) se centran en la practicidad (rendimiento, casos reales). (Mazzocca et al., 2024/2025; Ghodsi et al., 2024).

2.7.7. Gobernanza y cumplimiento (RGPD/eIDAS 2.0)

En el plano regulatorio, los trabajos exploran tensiones entre inmutabilidad y derechos (acceso/supresión) y comparan ZKP vs SD-JWT bajo eIDAS 2.0, proponiendo patrones de anclaje off-chain, revocación/expiración y roles claros de controllers/processors. (van Eerten et al., 2024; Shehu, 2024).

2.8. Brechas de conocimiento derivadas del estado del arte

Las brechas de conocimiento se presentan aquí como resultado del análisis crítico del estado del arte. La matriz de consistencia metodológica correspondiente se desarrolla en el Capítulo 3, debido a que allí se articulan formalmente problema, objetivos, hipótesis, variables, indicadores, técnicas e instrumentos.

Tabla 5. Brechas de conocimiento derivadas del estado del arte

Brecha identificada	Evidencia en el estado del arte	Consecuencia metodológica	Dimensión afectada	Respuesta del modelo propuesto
Fragmentación tecnológica	Blockchain, ZKP, cifrado homomórfico y ABAC suelen analizarse de forma aislada.	Comparar un modelo integrado frente a modelos base.	Privacidad y seguridad	Arquitectura integrada con ancla blockchain, divulgación selectiva, tratamiento cifrado y acceso adaptativo.
Riesgo de correlación	Las cadenas públicas y la reutilización de identificadores pueden exponer metadatos.	Medir no vinculabilidad y porcentaje de atributos divulgados.	Privacidad y soberanía digital	Uso de ZKP/BBS+ y minimización de atributos en la presentación de credenciales.
Interoperabilidad insuficiente	Los ecosistemas DID/VC presentan diferencias de métodos, formatos y wallets.	Evaluar compatibilidad con estándares y perfiles de intercambio.	Interoperabilidad	Alineación con DID/VC, OIDC4VCI/OIDC4VP y criterios de compatibilidad técnica.
Débil validación empírica	Varias propuestas se mantienen en el plano conceptual o prototípico.	Justificar un diseño cuasi-experimental con simulación controlada.	Validez metodológica	Comparación entre cuatro modelos mediante indicadores técnicos y normativos.
Escasa validación experta	La literatura técnica no siempre contrasta la	Incorporar juicio de expertos como	Pertinencia y viabilidad	Anexo de validación del modelo mediante rúbrica de expertos.

	viabilidad con criterio experto.	validación cualitativa.		

Fuente: Elaboración propia

Tabla 6. Articulación entre brechas de conocimiento

Brecha de conocimiento	**Objetivo relacionado**	**Relación con la hipótesis**
Riesgos de privacidad, exposición de metadatos y correlación de identidades en modelos DID/SSI.	Analizar los riesgos de privacidad y seguridad en sistemas actuales de identidad digital descentralizada.	Sustenta la necesidad de comprobar si el modelo propuesto mejora la privacidad y la seguridad.
Falta de integración entre blockchain, ZKP, cifrado homomórfico y control de acceso adaptativo.	Evaluar protocolos, estándares y marcos regulatorios relevantes.	Justifica la hipótesis de que una arquitectura integrada puede superar modelos aislados o básicos.
Limitaciones de interoperabilidad entre DID, VC, OAuth2, OpenID Connect, FIDO2, RGPD y eIDAS 2.0.	Evaluar protocolos, estándares y marcos regulatorios relevantes.	Sustenta la dimensión de interoperabilidad y cumplimiento de la hipótesis general.
Escasez de evaluaciones comparativas con métricas	Comparar el modelo propuesto con soluciones existentes.	Permite contrastar empíricamente si existen mejoras significativas frente a

técnicas, normativas y de usabilidad.		modelos centralizados y SSI básicos.
Falta de indicadores operativos para soberanía digital y no vinculabilidad.	Comparar mejoras en seguridad, privacidad, interoperabilidad y usabilidad.	Refuerza la necesidad de medir no vinculabilidad, divulgación de atributos y control del usuario como parte de la hipótesis.

Fuente: Elaboración propia

2.9. Síntesis integradora del estado del arte

Al revisar el estado del arte queda claro que los avances recientes en identidad digital descentralizada aportan sobre todo en tres frentes: interoperabilidad técnica, privacidad criptográfica y cumplimiento normativo. Estándares como DID/VC, VCDM 2.0, OIDC4VCI, OIDC4VP y SD-JWT VC facilitan que emisores, titulares y verificadores se entiendan entre sí; mecanismos como la divulgación selectiva, BBS+ y las pruebas de conocimiento cero refuerzan la minimización de datos y la no vinculabilidad; y marcos como el RGPD y el eIDAS 2.0 empujan el diseño hacia arquitecturas más responsables y verificables.

El problema es que esos avances siguen bastante fragmentados. Hay propuestas centradas en blockchain —desde visiones amplias de su aplicación económica y social (Swan, 2015) hasta arquitecturas puntuales para descentralizar el control de datos personales (Zyskind et al., 2015)—; otras se centran en credenciales verificables, algunas en pruebas de conocimiento cero y otras en cumplimiento normativo. Pero son pocos los modelos que juntan todo esto y lo evalúan de forma comparativa con métricas técnicas, regulatorias y de usabilidad. Esa falta de integración impide saber si una arquitectura descentralizada puede realmente dar, al mismo tiempo,

privacidad, seguridad, interoperabilidad, soberanía digital y un desempeño operacional aceptable.

Sobre esa base, esta investigación propone un modelo avanzado de identidad digital descentralizada que junta cinco piezas: blockchain como ancla de confianza, pruebas de conocimiento cero para la divulgación selectiva, cifrado homomórfico para procesar atributos de forma segura, control de acceso adaptativo basado en atributos, y una matriz de evaluación alineada con principios de privacidad y cumplimiento normativo. El estudio no se queda entonces en describir el estado del arte: plantea una contribución evaluativa, comparativa y cuasi-experimental que busca comprobar, empíricamente, el impacto del modelo propuesto frente a las soluciones tradicionales y las implementaciones básicas de identidad autosoberana.

2.10. Aportes teóricos, metodológicos y normativos derivados del estado del arte

2.10.1. Estandarización e interoperabilidad (VCDM 2.0, OID4VCI/OID4VP y SD-JWT VC)

En 2024–2025 se consolidó un “pivote” de interoperabilidad que conecta SSI con infraestructuras Web2 existentes. Primero, el W3C Verifiable Credentials Data Model 2.0 (VCDM 2.0) alcanzó estatus de estándar, reforzando un modelo de datos independiente de los mecanismos de aseguramiento (LD-Proofs, JWT, BBS+, SD-JWT), lo que facilita composiciones y perfiles interoperables sin rehacer el *stack* de datos. Esto es clave para ecosistemas multi-jurisdiccionales y multi-proveedor donde distintos dominios requieren distintas suites criptográficas.

Segundo, la familia OpenID for Verifiable Credentials (OID4VC) maduró en sus flujos de emisión (OIDC4VCI) y presentación (OIDC4VP), describiendo perfiles y metadatos que permiten integrar wallets y verificadores en arquitecturas OIDC con mínima fricción; versiones recientes de las especificaciones clarifican *holder binding*, metadatos del emisor y

compatibilidad con diferentes formatos de credenciales. Esto acelera pilotos empresariales y gubernamentales al reutilizar componentes probados de OIDC/OAuth2.

Tercero, el IETF avanzó SD-JWT y SD-JWT-VC, llevando divulgación selectiva en formato JWT a entornos donde JSON/JWT es el sustrato dominante (móvil, *federation stacks*), con definiciones de metadatos, *key binding* y estatus (revocación) propias del formato. Para implementadores, esto reduce la brecha entre "lo que ya existe" en Web2 y "lo que se necesita" para minimizar datos en SSI.

Aportación a la tesis. Este frente te permite definir un perfil interoperable mínimo (VCDM 2.0 + OIDC4VCI/OIDC4VP + SD-JWT VC) y compararlo con alternativas LD-Proofs/BBS+. Propones métricas reproducibles: (i) latencia P95 de emisión/presentación, (ii) tamaño de VP/overhead de transporte, (iii) tasa de verificación cruzada *wallet* ↔ *verifier* heterogéneos, y (iv) cobertura de minimización (claims revelados vs. requeridos). Con ello, podrás demostrar empíricamente qué combinación ofrece el mejor equilibrio entre interoperabilidad y privacidad en contextos regulados.

2.10.2. Divulgación selectiva y no-vinculabilidad con BBS+ (Data Integrity Cryptosuite)

El W3C Data Integrity BBS Cryptosuites v1.0 invita implementaciones y pruebas de interoperabilidad como Candidate Recommendation Snapshot, destacando dos propiedades cruciales para SSI: divulgación selectiva y pruebas derivadas no vinculables (unlinkable derived proofs). BBS+ habilita demostrar subconjuntos de atributos sin exponer el resto, mitigando correlaciones entre verificaciones repetidas (mismo titular en distintos dominios) y alineándose con *privacy by design*. La especificación y las comunicaciones de W3C fijan un camino claro de adopción y de *conformance* con *test vectors* públicos.

El acoplamiento VCDM 2.0 + BBS+ es especialmente útil cuando la *no-vinculabilidad fuerte* es un requisito (salud, finanzas, identidad legal): el modelo de datos 2.0 no fuerza un único mecanismo criptográfico, por lo que es factible ofrecer perfiles duales (p. ej., BBS+ para LD-Proofs y SD-JWT para entornos JWT), maximizando compatibilidad sin sacrificar privacidad. Para arquitecturas con DIDs pareados y rotación, BBS+ actúa como columna técnica que reduce la exposición de metadatos y el riesgo de correlación en redes o verificadores coludidos.

Aportación a la tesis. Este tema habilita una operacionalización rigurosa de la "soberanía" y la "no-vinculabilidad". Podrás definir y medir: (i) *índice de vinculabilidad* entre presentaciones (antes/después de BBS+), (ii) *entropía de DIDs pareados* bajo rotación controlada, (iii) *volumen de datos revelados/transacción* y (iv) *costo/verificación* de pruebas. Con un *prototype-in-the-loop*, contrastas BBS+ frente a SD-JWT/AnonCreds y cuantificas el beneficio de políticas de minimización por defecto (pairwise DIDs, relays/mediación, *log hygiene* de verificadores). Esto provee evidencia empírica para tu propuesta de arquitectura centrada en privacidad.

2.10.3. Marco regulatorio y despliegue: eIDAS 2.0 y la EU Digital Identity Wallet (EUDI)

En 2024 se adoptó el Reglamento (UE) 2024/1183 (eIDAS 2.0), que establece el marco para la EU Digital Identity Wallet (EUDI) y fija obligaciones de reconocimiento, certificación y estados de conformidad. En diciembre de 2024 se aprobó una primera ronda de actos de ejecución y, crucialmente, en mayo de 2025 se publicó una nueva ronda de reglamentos de implementación en el Diario Oficial, con entrada en vigor 20 días después. Este calendario normativo transforma SSI de "potencial" a programa de despliegue con reglas comunes, *toolbox* y arquitectura de referencia para que los Estados miembros desarrollen wallets interoperables y *privacy-enhancing* aceptadas por *relying parties* registradas.

Para proyectos académicos y pilotos, esto implica alinear decisiones de diseño (anclaje *off-chain*, mecanismos de divulgación selectiva/no-vinculabilidad, revocación/expiración) con perfiles de conformidad y evaluaciones de seguridad/privacidad. Además, eIDAS 2.0 exige clarificar roles y responsabilidades (emisor, verificador, proveedor de wallet, operador de *ledger*) y medir atributos de "alto nivel de garantía". La referencia pública a listas de *wallets* certificadas y a estándares de interoperabilidad proporciona trazabilidad regulatoria que tu tesis puede aprovechar como mecanismo de validación externa.

Aportación a la tesis. Este frente te permite construir una matriz de trazabilidad regulatoria que vincule: (i) métricas técnicas (latencia, tamaño de prueba, tasa de verificación, *unlinkability*), (ii) controles de minimización/limitación de finalidad y (iii) requisitos de eIDAS 2.0/EUDI (revocación, expiración, aceptación por *relying parties* registradas, niveles de garantía). Con ello, tu modelo propuesto (hashes/schemas/status *on-chain*, ZKP/BBS+, SD-JWT u OIDC4VP/4VCI para compatibilidad) se valida no solo técnicamente, sino también jurídica y operacionalmente frente a una norma de alcance regional.

2.11. Implicaciones del estado del arte para el modelo propuesto

Los tres frentes recientes proporcionan artefactos medibles:

- perfiles interoperables (VCDM 2.0 + OID4VCI/OID4VP + SD-JWT VC)
- mecanismos de privacidad fuerte (BBS+)
- criterios de conformidad (eIDAS 2.0/EUDI).

Esto habilita un marco de evaluación comparativa *end-to-end* con indicadores de rendimiento, minimización y cumplimiento.

Evaluar. Con *prototype-in-the-loop* podrás contrastar JWT-centric vs. LD-Proofs-centric bajo cargas realistas y reportar tasa de verificación cruzada y coste de pruebas en diferentes

wallets/verifiers; además, podrás mapear resultados a obligaciones eIDAS 2.0 para mostrar *fitness for regulation*.

Crear. Sobre esta base, tu modelo avanzado integra: (i) anclaje *on-chain* mínimo (hashes/schemas/status) + off-chain de datos personales; (ii) BBS+ para no-vinculabilidad y divulgación selectiva; (iii) OID4VCI/OID4VP/SD-JWT para compatibilidad con OIDC; (iv) ABAC/PBAC con políticas de minimización por defecto; y (v) una matriz de conformidad eIDAS 2.0. El resultado es una arquitectura auditable, portable e interoperable que optimiza privacidad sin penalizar rendimiento ni adopción.

2.12. Marco teórico-conceptual integrado

La identidad digital descentralizada constituye un campo de estudio interdisciplinario que articula conceptos provenientes de la informática, la criptografía, la seguridad de la información, la protección de datos personales, la gobernanza digital y la teoría de la confianza. A diferencia de los modelos tradicionales de identidad, en los que una autoridad central conserva, administra y valida las credenciales del usuario, los modelos descentralizados proponen una redistribución del control mediante identificadores descentralizados, credenciales verificables y mecanismos criptográficos de comprobación. Esta transformación no solo implica un cambio tecnológico, sino también una modificación profunda en la forma de concebir la confianza, la autonomía del usuario y la legitimidad de las transacciones digitales (Mühle et al., 2018; Goodell & Aste, 2019).

Desde el enfoque clásico, la identidad digital se ha basado en registros centralizados administrados por gobiernos, bancos, universidades, empresas tecnológicas o proveedores de servicios. En estos esquemas, el usuario depende de una entidad externa para demostrar quién es, acceder a servicios o validar atributos personales. Aunque este modelo ofrece eficiencia

operativa, también genera riesgos significativos, entre ellos la concentración de datos, la exposición masiva ante brechas de seguridad, la dependencia de terceros y la pérdida de control del titular sobre sus credenciales. En este sentido, la identidad digital centralizada reproduce una relación asimétrica entre el proveedor y el usuario, donde la confianza se deposita principalmente en la institución que almacena y procesa la información.

La identidad digital descentralizada surge como una respuesta a estas limitaciones. Su fundamento se encuentra en la posibilidad de que el usuario gestione sus propios identificadores y credenciales sin depender de un repositorio central. Los identificadores descentralizados permiten establecer relaciones verificables entre titulares, emisores y verificadores, mientras que las credenciales verificables permiten representar declaraciones digitales firmadas criptográficamente. De esta manera, el titular puede presentar evidencia de un atributo sin que el verificador necesite consultar permanentemente a la entidad emisora. Este enfoque fortalece la portabilidad de las credenciales, reduce la exposición innecesaria de datos y promueve una arquitectura más alineada con el principio de soberanía digital (Longley & Reed, 2020; W3C, 2023).

La identidad autosoberana, o identidad autosoberana, constituye uno de los enfoques más relevantes dentro de este campo. Este paradigma sostiene que el usuario debe conservar el control principal sobre sus credenciales, decidir qué atributos comparte, con quién los comparte y bajo qué condiciones. La soberanía digital no significa ausencia de regulación o de emisores confiables, sino redistribución del control hacia el titular de la identidad. En consecuencia, el usuario deja de ser un sujeto pasivo dentro del ecosistema digital y se convierte en un actor con mayor capacidad para administrar sus datos, consentir su uso y limitar su exposición (Reed et al., 2016; Reece et al., 2022).

No obstante, la descentralización por sí sola no garantiza privacidad. Una arquitectura basada en blockchain puede ofrecer trazabilidad, integridad y resistencia a manipulaciones, pero también puede generar riesgos si expone metadatos, identificadores persistentes o patrones de interacción. Por ello, la identidad descentralizada requiere mecanismos criptográficos complementarios que permitan verificar información sin revelar datos sensibles. En este punto adquieren relevancia las pruebas de conocimiento cero, las cuales permiten demostrar la validez de una afirmación sin revelar el contenido completo que la sustenta. Por ejemplo, un usuario puede demostrar que cumple una condición, como ser mayor de edad o pertenecer a una institución, sin revelar su fecha de nacimiento completa o todos sus datos personales (Schanzenbach et al., 2019; Zhou et al., 2020).

El cifrado homomórfico constituye otro componente importante dentro del marco conceptual de esta investigación. Su valor radica en la posibilidad de realizar operaciones sobre datos cifrados sin necesidad de descifrarlos. Aunque su implementación puede implicar mayores costos computacionales, representa una alternativa relevante para escenarios donde la confidencialidad debe mantenerse durante el procesamiento de información sensible. En sistemas de identidad digital, este tipo de cifrado puede contribuir a verificar atributos o ejecutar reglas de decisión sin exponer directamente los datos personales del titular.

El control de acceso adaptativo basado en atributos también forma parte del núcleo conceptual del modelo propuesto. A diferencia de los esquemas rígidos basados únicamente en roles, el control de acceso basado en atributos permite tomar decisiones dinámicas considerando características del usuario, contexto de la solicitud, nivel de riesgo, tipo de recurso y políticas de seguridad. Esta capacidad resulta especialmente importante en entornos descentralizados, donde

los usuarios, emisores y verificadores pueden pertenecer a organizaciones distintas y operar bajo condiciones cambiantes (Hu et al., 2015).

2.13. Marco histórico

La evolución histórica de la identidad digital puede comprenderse como una transición progresiva desde modelos centralizados hacia modelos federados y, posteriormente, hacia arquitecturas descentralizadas y autosoberanas. Esta evolución responde a la necesidad de resolver problemas recurrentes relacionados con autenticación, confianza, interoperabilidad, protección de datos y control del usuario sobre su información personal. Cada etapa ha aportado soluciones relevantes, pero también ha generado limitaciones que justifican la búsqueda de modelos más seguros y orientados a la privacidad.

En una primera etapa, la identidad digital se desarrolló bajo modelos centralizados. En estos esquemas, una entidad única, como una institución pública, banco, universidad, empresa o proveedor tecnológico, almacena y administra las credenciales de los usuarios. El acceso a servicios digitales depende de la validación realizada por dicha entidad. Este enfoque permitió organizar la autenticación en sistemas cerrados y facilitó la gestión inicial de usuarios, contraseñas y permisos. Sin embargo, también creó puntos únicos de fallo y elevó el riesgo asociado a la concentración de datos personales. Una brecha de seguridad en un sistema centralizado puede comprometer millones de registros simultáneamente, afectando la privacidad, la seguridad y la confianza de los usuarios (Mühle et al., 2018; Bonneau et al., 2012).

El modelo centralizado también consolidó una relación de dependencia entre el usuario y el proveedor de identidad. En la práctica, el usuario no controla plenamente sus credenciales ni decide de forma autónoma cómo se comparten sus datos. Además, los proveedores pueden recopilar, procesar y correlacionar información de múltiples interacciones, generando riesgos de

vigilancia, perfilamiento y uso secundario de datos. Estas limitaciones evidenciaron la necesidad de modelos capaces de distribuir la confianza y reducir la exposición de información sensible.

La segunda etapa corresponde al desarrollo de la identidad federada. Este modelo buscó mejorar la experiencia del usuario mediante la reutilización de credenciales entre diferentes servicios. Protocolos como SAML, OAuth2 y OpenID Connect permitieron que un usuario accediera a varias plataformas utilizando una identidad emitida por un proveedor confiable. Este enfoque redujo la necesidad de mantener múltiples credenciales y facilitó la interoperabilidad entre sistemas. OAuth2, por ejemplo, se consolidó como un estándar para autorización delegada, permitiendo que una aplicación acceda a ciertos recursos sin que el usuario entregue directamente sus credenciales completas (Hardt, 2012).

Aunque la identidad federada representó un avance frente a la fragmentación de credenciales, no resolvió completamente el problema de la dependencia de terceros. En muchos casos, el usuario continuó dependiendo de grandes proveedores de identidad para acceder a servicios digitales. Esto mantuvo riesgos de concentración, perfilamiento y pérdida de autonomía. Además, la federación no garantiza necesariamente la minimización de datos, ya que los atributos compartidos pueden exceder la información estrictamente necesaria para una transacción determinada (Reece et al., 2022).

La tercera etapa está representada por la identidad digital descentralizada y la identidad autosoberana. Este enfoque se consolidó con el desarrollo de tecnologías blockchain, identificadores descentralizados y credenciales verificables. A diferencia de los modelos centralizados y federados, la identidad descentralizada busca que el usuario tenga mayor control sobre sus credenciales y pueda presentarlas ante terceros sin depender constantemente de un

proveedor de identidad. El emisor continúa siendo relevante, porque firma o certifica una credencial, pero el titular adquiere mayor autonomía para almacenarla, gestionarla y presentarla.

Blockchain contribuyó a este cambio al proporcionar una infraestructura de confianza distribuida, capaz de registrar anclajes criptográficos, esquemas o evidencias verificables sin requerir una autoridad central única. Sin embargo, su uso en identidad digital debe ser cuidadoso, porque la transparencia e inmutabilidad de la cadena pueden generar tensiones con la privacidad si se almacenan datos personales o metadatos sensibles. Por ello, las arquitecturas modernas tienden a separar los datos personales de la cadena y utilizar blockchain únicamente como mecanismo de anclaje, trazabilidad o verificación (Goodell & Aste, 2019; Zhou et al., 2020).

En paralelo, los estándares de identificadores descentralizados y credenciales verificables impulsados por el W3C han permitido estructurar de manera más formal los componentes de la identidad descentralizada. Los DID permiten identificar entidades sin depender de registros centralizados, mientras que las VC permiten representar afirmaciones verificables sobre un sujeto. Esta combinación facilita escenarios de emisión, presentación y verificación de credenciales en ecosistemas distribuidos, interoperables y potencialmente compatibles con marcos regulatorios emergentes (Longley & Reed, 2020; W3C, 2023).

La evolución histórica demuestra que cada etapa respondió a problemas no resueltos por la anterior. Los modelos centralizados ofrecieron simplicidad, pero concentraron riesgos. Los modelos federados mejoraron la interoperabilidad, pero mantuvieron dependencia de proveedores. Los modelos descentralizados fortalecen el control del usuario, pero introducen desafíos técnicos relacionados con escalabilidad, revocación, interoperabilidad y protección frente a correlación. En consecuencia, la presente investigación se ubica en esta tercera etapa

evolutiva y propone avanzar hacia un modelo híbrido que combine descentralización, privacidad criptográfica, control adaptativo y cumplimiento normativo.

2.14. Marco referencial

El marco referencial de esta investigación se sustenta en enfoques teóricos y normativos que permiten comprender la identidad digital descentralizada no solo como una solución tecnológica, sino como un sistema socio-técnico orientado a proteger la privacidad, distribuir la confianza y fortalecer la autonomía del usuario. En este sentido, se consideran tres ejes principales: privacidad por diseño, consentimiento informado y confianza digital distribuida.

El principio de privacidad por diseño plantea que la protección de datos personales debe integrarse desde la concepción inicial de un sistema, y no incorporarse como un mecanismo correctivo posterior. Este enfoque exige que la arquitectura tecnológica limite la recolección de datos, reduzca la exposición innecesaria de atributos y permita que la privacidad sea una configuración predeterminada. En los sistemas de identidad digital descentralizada, este principio resulta fundamental porque las credenciales pueden circular entre múltiples emisores, titulares y verificadores, lo que incrementa la necesidad de controlar la información revelada en cada interacción (Cavoukian, 2010), en consonancia con la terminología clásica sobre anonimato, seudonimato y no vinculabilidad que sustenta el vocabulario técnico de la privacidad (Pfitzmann & Hansen, 2010). Esta necesidad se agudiza en contextos de datos masivos, donde la agregación de información aparentemente inocua puede erosionar el control efectivo del usuario sobre su perfil digital (Tene & Polonetsky, 2013).

Desde esta perspectiva, la minimización de datos se convierte en un criterio central. Un sistema de identidad digital no debería exigir al usuario revelar más información de la estrictamente necesaria para cumplir una finalidad concreta. Por ejemplo, para demostrar

mayoría de edad no debería requerirse revelar nombre completo, fecha exacta de nacimiento, dirección u otros atributos personales. Las pruebas de conocimiento cero y los mecanismos de divulgación selectiva permiten operacionalizar este principio, ya que posibilitan validar condiciones específicas sin exponer el conjunto completo de datos personales (Schanzenbach et al., 2019; Zhou et al., 2020).

El segundo eje referencial corresponde al consentimiento informado. En los modelos tradicionales, el consentimiento suele expresarse mediante formularios extensos o aceptaciones generales, sin que el usuario tenga control granular sobre cada atributo compartido. En cambio, los modelos basados en DID y credenciales verificables permiten avanzar hacia un consentimiento más específico, contextual y verificable. El usuario puede seleccionar qué credenciales presentar, qué atributos revelar y ante qué verificador hacerlo. Este enfoque fortalece la capacidad de decisión del titular y reduce la exposición innecesaria de información (Longley & Reed, 2020; OpenID Foundation, 2024).

El consentimiento informado también se relaciona con la transparencia y la trazabilidad. Para que el usuario ejerza un control real sobre su identidad digital, debe comprender qué información se solicita, con qué finalidad, por cuánto tiempo será utilizada y bajo qué condiciones podrá ser revocada o actualizada. En este sentido, las billeteras digitales, los protocolos de presentación de credenciales y los mecanismos de revocación constituyen elementos técnicos relevantes para garantizar un consentimiento más efectivo, entendidos como aplicaciones concretas de las tecnologías de mejora de la privacidad descritas en la literatura sobre ética e ingeniería de sistemas (van Sabben & van den Hoven, 2018).

El tercer eje corresponde a la confianza digital distribuida. En los modelos centralizados, la confianza se deposita en una institución que administra la identidad. En los modelos

descentralizados, la confianza se desplaza hacia un conjunto de mecanismos criptográficos, estándares técnicos, reglas de gobernanza y evidencias verificables. Esto no significa que desaparezcan las instituciones, sino que su papel cambia: los emisores certifican atributos, los titulares gestionan sus credenciales y los verificadores comprueban la validez de las presentaciones mediante pruebas criptográficas (Goodell & Aste, 2019; Mühle et al., 2018). Esta discusión se enmarca en un debate más amplio sobre la tensión entre los mercados de datos personales y la privacidad individual, evidenciada desde los primeros análisis económicos de la información personal como bien transable (Laudon, 1996).

La confianza digital distribuida también requiere interoperabilidad. Un modelo de identidad descentralizada solo puede ser viable si las credenciales emitidas por una entidad pueden ser entendidas, procesadas y verificadas por múltiples actores. Por ello, estándares como DID, VC, OIDC4VCI, OIDC4VP y BBS+ resultan relevantes para evitar soluciones aisladas o incompatibles. La interoperabilidad permite que la soberanía digital no quede limitada a un ecosistema cerrado, sino que pueda aplicarse en contextos gubernamentales, financieros, académicos, sanitarios y empresariales (W3C, 2023; OpenID Foundation, 2024), en sintonía con modelos emergentes de colaboración de datos entre instituciones que buscan equilibrar apertura e intercambio de información con la protección de la privacidad (Verhulst, 2018).

A partir de estos enfoques, el marco referencial de esta tesis permite evaluar el modelo propuesto desde una perspectiva integral. No basta con que una arquitectura sea técnicamente funcional; también debe proteger la privacidad desde el diseño, permitir consentimiento granular, reducir la dependencia de terceros, garantizar verificabilidad y mantener compatibilidad con estándares. Por ello, la propuesta se orienta a integrar mecanismos criptográficos, control

adaptativo y evaluación normativa dentro de una arquitectura de identidad digital descentralizada.

2.15. Marco legal

El marco legal constituye un componente esencial para evaluar la viabilidad de cualquier modelo de identidad digital descentralizada. La gestión de credenciales, atributos y datos personales no puede analizarse únicamente desde una perspectiva técnica, debido a que involucra derechos fundamentales relacionados con privacidad, protección de datos, consentimiento, portabilidad, transparencia y control del usuario. Por esta razón, la presente investigación considera como referentes normativos principales el Reglamento General de Protección de Datos, eIDAS 2.0, la European Digital Identity Wallet y la norma ISO/IEC 29100.

El Reglamento General de Protección de Datos establece principios fundamentales para el tratamiento de información personal, entre ellos licitud, lealtad, transparencia, minimización de datos, limitación de finalidad, exactitud, limitación del plazo de conservación, integridad y confidencialidad. Estos principios son directamente aplicables a los sistemas de identidad digital, ya que dichos sistemas procesan información altamente sensible relacionada con la identificación, autenticación y autorización de personas. En consecuencia, una arquitectura de identidad descentralizada debe diseñarse de manera que reduzca la exposición de datos, evite tratamientos innecesarios y permita al usuario conservar un control efectivo sobre sus credenciales (European Data Protection Board, 2020).

Uno de los principios más relevantes para esta investigación es la minimización de datos. Este principio establece que solo deben tratarse los datos necesarios para una finalidad específica. En los modelos centralizados, la verificación de identidad suele implicar la entrega de múltiples atributos, incluso cuando solo se requiere comprobar una condición concreta. Frente a

ello, las credenciales verificables y las pruebas de conocimiento cero permiten construir mecanismos de verificación más compatibles con la minimización, al permitir demostrar atributos sin revelar información adicional. De esta manera, la privacidad no depende únicamente de políticas organizacionales, sino también de propiedades técnicas incorporadas en la arquitectura del sistema.

Otro aspecto relevante es la tensión entre blockchain y el derecho de supresión. Debido a la inmutabilidad de los registros distribuidos, almacenar datos personales directamente en una cadena de bloques puede entrar en conflicto con derechos vinculados a rectificación, cancelación o supresión. Para mitigar este riesgo, las arquitecturas modernas recomiendan evitar la inclusión de datos personales en la cadena y utilizar blockchain únicamente para registrar hashes, esquemas, identificadores o evidencias criptográficas no reversibles. Esta estrategia permite conservar trazabilidad e integridad sin comprometer de manera directa los derechos de protección de datos (van Eerten et al., 2024; European Union Agency for Cybersecurity, 2021).

El Reglamento eIDAS 2.0 y la European Digital Identity Wallet refuerzan la relevancia jurídica de los sistemas de identidad digital interoperables. Este marco busca establecer condiciones para que los ciudadanos puedan utilizar billeteras digitales reconocidas, seguras y compatibles en distintos Estados y servicios. Para una investigación sobre identidad descentralizada, eIDAS 2.0 resulta especialmente importante porque introduce exigencias relacionadas con confianza, interoperabilidad, niveles de garantía, aceptación transfronteriza y control del usuario sobre sus atributos digitales (European Commission, 2023). Este interés no se limita al contexto europeo: agencias gubernamentales en otras regiones han explorado igualmente el potencial de la identidad descentralizada para la gestión de confianza en servicios públicos (U.S. Department of Homeland Security, 2018).

La European Digital Identity Wallet plantea un escenario en el que los usuarios pueden almacenar y presentar credenciales digitales en contextos públicos y privados. Esto exige que los modelos de identidad digital combinen seguridad técnica, protección de datos, facilidad de uso y reconocimiento jurídico. Por tanto, la propuesta de esta tesis se alinea con dicha tendencia al integrar mecanismos de divulgación selectiva, control de acceso adaptativo y verificación criptográfica para reducir la exposición de información personal.

La norma ISO/IEC 29100 aporta un marco internacional de privacidad que complementa los enfoques regulatorios anteriores. Esta norma establece principios como consentimiento, legitimidad, limitación de recolección, minimización, exactitud, apertura, participación individual, responsabilidad y seguridad de la información. Su valor dentro de esta investigación radica en que permite traducir principios de privacidad en criterios evaluables para el modelo propuesto (ISO/IEC, 2011). Estos principios convergen con marcos previos de referencia internacional, como el marco de privacidad de la OCDE (OECD, 2013), y se complementan con guías técnicas específicas para identidad digital, entre ellas las directrices de identidad digital del NIST, que establecen niveles de garantía para la verificación de identidad y autenticación (NIST, 2020).

En conjunto, el marco legal evidencia que la identidad digital descentralizada debe diseñarse con una visión técnica y normativa integrada. No basta con implementar blockchain, DID o credenciales verificables; es necesario asegurar que la arquitectura respete principios de minimización, consentimiento, trazabilidad, revocabilidad, interoperabilidad y control del usuario. Por ello, el modelo propuesto evita almacenar datos personales directamente en cadena, utiliza mecanismos criptográficos de divulgación selectiva y evalúa su desempeño frente a criterios normativos derivados de RGPD, eIDAS 2.0 e ISO/IEC 29100.

2.16. Categorías conceptuales para la operacionalización

Los conceptos clave de esta investigación delimitan el alcance técnico, metodológico y normativo del modelo propuesto. Debido a que la identidad digital descentralizada integra tecnologías y enfoques de distintas áreas, resulta necesario precisar los términos que estructuran el análisis: identificadores descentralizados, credenciales verificables, identidad autosoberana, blockchain, pruebas de conocimiento cero, cifrado homomórfico, no vinculabilidad, interoperabilidad y control de acceso adaptativo.

Los identificadores descentralizados, conocidos como DID, son identificadores digitales diseñados para no depender de una autoridad central. A diferencia de los identificadores tradicionales, que suelen estar controlados por una organización específica, los DID permiten que una entidad genere, administre y utilice identificadores verificables dentro de un ecosistema distribuido. Su función principal es permitir relaciones confiables entre titulares, emisores y verificadores sin requerir un registro central único (Longley & Reed, 2020), retomando principios tempranos de arquitecturas de identificadores digitales persistentes e independientes de una ubicación de red específica (Kahn, 2000).

Las credenciales verificables son declaraciones digitales firmadas criptográficamente por un emisor. Estas credenciales pueden representar atributos como identidad, edad, afiliación institucional, certificaciones académicas, licencias profesionales o autorizaciones específicas. Su valor radica en que pueden ser presentadas por el titular y verificadas por un tercero sin necesidad de consultar permanentemente al emisor. Esto mejora la portabilidad, reduce dependencia institucional y facilita procesos de verificación más eficientes (W3C, 2023), de acuerdo con el modelo de datos estandarizado para su representación, intercambio y verificación (Sporny et al., 2019).

La identidad autosoberana se refiere al enfoque según el cual el titular conserva el control principal sobre sus credenciales y atributos digitales. Este modelo busca que el usuario pueda almacenar sus credenciales en una billetera digital, decidir qué información presentar y reducir su dependencia de proveedores centralizados de identidad. La SSI no elimina la necesidad de emisores confiables, pero redistribuye el control operativo hacia el usuario, fortaleciendo la autonomía y la soberanía digital (Reed et al., 2016; Reece et al., 2022).

Blockchain es una tecnología de registro distribuido que permite almacenar información de manera inmutable, verificable y resistente a manipulaciones. En identidad digital descentralizada, su uso debe ser cuidadosamente delimitado. No se recomienda almacenar datos personales directamente en la cadena; en cambio, puede emplearse para registrar anclajes criptográficos, esquemas de credenciales, estados de revocación o evidencias verificables. De esta manera, blockchain actúa como una capa de confianza sin convertirse en un repositorio de información sensible (Goodell & Aste, 2019; Zhou et al., 2020).

Las pruebas de conocimiento cero son mecanismos criptográficos que permiten demostrar que una afirmación es verdadera sin revelar la información subyacente. En el contexto de identidad digital, estas pruebas permiten validar atributos personales sin exponer datos completos. Por ejemplo, una persona puede demostrar que cumple un requisito sin revelar todos los atributos de su credencial. Esto resulta fundamental para la minimización de datos, la privacidad por diseño y la reducción de riesgos de correlación (Schanzenbach et al., 2019).

El cifrado homomórfico permite realizar operaciones sobre datos cifrados sin necesidad de descifrarlos. Aunque su implementación puede ser costosa en términos computacionales, su incorporación en modelos de identidad digital resulta relevante para escenarios donde se requiere procesar información sensible sin exponerla. Este mecanismo complementa las pruebas de

conocimiento cero al ofrecer una capa adicional de confidencialidad durante el tratamiento de atributos (Zhou et al., 2020).

La no vinculabilidad es la propiedad mediante la cual distintas transacciones, presentaciones o verificaciones no pueden asociarse fácilmente a un mismo usuario. En identidad digital descentralizada, esta propiedad es esencial porque evita que verificadores o terceros puedan reconstruir perfiles del usuario a partir de sus interacciones, un riesgo identificado tempranamente en la literatura sobre privacidad como agregación y vigilancia de datos personales (Solove, 2006). La no vinculabilidad puede fortalecerse mediante DID pareados, rotación de identificadores, divulgación selectiva y pruebas criptográficas no correlacionables.

La interoperabilidad se refiere a la capacidad del modelo para operar con distintos estándares, plataformas, billeteras, emisores y verificadores. En un ecosistema de identidad digital, la interoperabilidad es fundamental para evitar dependencias de un único proveedor o plataforma. Estándares como DID, VC, OIDC4VCI, OIDC4VP y BBS+ permiten avanzar hacia sistemas más compatibles y transferibles entre contextos tecnológicos y jurisdiccionales (OpenID Foundation, 2024; W3C, 2023).

Finalmente, el control de acceso adaptativo basado en atributos permite tomar decisiones de autorización considerando características del usuario, atributos de la credencial, contexto de la solicitud, nivel de riesgo y políticas institucionales. A diferencia de los modelos basados únicamente en roles, el enfoque ABAC proporciona mayor granularidad y flexibilidad. En esta investigación, este componente es clave porque permite ajustar las condiciones de acceso sin sacrificar privacidad ni usabilidad (Hu et al., 2015).

En síntesis, estos conceptos conforman la base técnica y teórica del modelo propuesto. La investigación no analiza DID, SSI, blockchain, ZKP, cifrado homomórfico y ABAC como

elementos aislados, sino como componentes de una arquitectura integrada orientada a mejorar la privacidad, la seguridad, la interoperabilidad, la usabilidad y la soberanía digital.

2.17. Conexión metodológica, brechas y proyección investigativa

En el desarrollo de una investigación doctoral resulta imprescindible trascender la simple descripción de tecnologías y marcos normativos. El análisis profundo de las arquitecturas de identidad digital descentralizada, de los protocolos criptográficos asociados y de las implicaciones legales permite identificar tanto sus fortalezas como sus limitaciones. A partir de esta base, la comparación crítica de distintos modelos y experiencias (como Hyperledger Indy, Sovrin, Civic o Microsoft Entra) se convierte en un ejercicio orientado a establecer criterios claros de privacidad, interoperabilidad y usabilidad.

Este proceso no se limita a una evaluación técnica; supone también reconocer los vacíos que persisten y las tensiones que se generan entre la innovación tecnológica y las exigencias regulatorias. En ese tránsito, la investigación doctoral se orienta hacia la creación de una propuesta novedosa, capaz de integrar de forma coherente blockchain, pruebas de conocimiento cero, cifrado homomórfico y mecanismos de control de acceso adaptativo. Con ello no solo se contribuye al avance del conocimiento, sino que se sientan las bases para soluciones prácticas que potencien la seguridad, la privacidad y la soberanía digital de los usuarios.

3. Propuesta metodológica

3.1. Enfoque metodológico

El enfoque mixto de esta investigación funciona como un diseño convergente: los datos cuantitativos y cualitativos se recogen, se analizan y se cruzan para responder al mismo problema. Lo cuantitativo mide qué tan bien funciona el modelo mediante indicadores técnicos y normativos; lo cualitativo interpreta si tiene sentido conceptual, jurídico y metodológico, apoyándose en análisis documental y en el juicio de expertos. Esa integración se logra por triangulación: se cruzan los resultados experimentales con la evidencia documental y con el criterio experto para ver si la propuesta es coherente y viable (Creswell & Plano Clark, 2018; Hernández Sampieri, 2021).

Concretamente, esto se traduce en tres tareas: cuantificar las mejoras en privacidad, seguridad, interoperabilidad, usabilidad y soberanía digital; interpretar esas mejoras a la luz de estándares, regulaciones y literatura especializada; y validar si el modelo propuesto es suficiente, con criterios técnicos, documentales y de expertos.

El estudio adopta, entonces, un enfoque mixto de carácter aplicado, explicativo y tecnológico, pensado para validar empíricamente un modelo híbrido de identidad digital descentralizada que combina blockchain, pruebas de conocimiento cero (ZKP), cifrado homomórfico y control de acceso adaptativo (ABAC). Esto permite mirar la identidad digital descentralizada desde dos ángulos: uno técnico y medible (rendimiento, latencia, exposición de datos, interoperabilidad, eficiencia criptográfica) y otro cualitativo y epistémico, centrado en la soberanía digital, la confianza distribuida, la ética de la privacidad y el cumplimiento normativo internacional (RGPD, eIDAS 2.0, ISO/IEC 29100).

Dicho de otra forma, el enfoque mixto permite triangular métodos cuantitativos —que miden, validan y comparan resultados experimentales— con métodos cualitativos, que aportan la lectura contextual, epistemológica y social de esos mismos resultados (Creswell & Plano Clark, 2018). La investigación no se queda entonces en medir el desempeño técnico del modelo;

también mira sus implicaciones de fondo: cómo cambia el concepto de identidad, qué formas de confianza aparecen en entornos distribuidos, y de qué manera las tecnologías descentralizadas modifican la relación entre individuo, institución y datos personales (Goodell & Aste, 2019).

El componente cuantitativo se justifica, sencillamente, porque hace falta contrastar la hipótesis general sobre el impacto del modelo propuesto en la privacidad, la seguridad, la interoperabilidad, la usabilidad y la soberanía digital de los sistemas de identidad.

El análisis cuantitativo, en concreto, se apoya en estadística descriptiva y comparativa, buscando relaciones de causalidad y correlación entre las variables independientes —blockchain, ZKP, cifrado homomórfico y políticas ABAC— y las dependientes —privacidad, seguridad, soberanía digital, usabilidad e interoperabilidad—. Este componente empírico se desarrolla mediante simulaciones computacionales y pruebas de laboratorio, buscando demostrar mejoras significativas en la no vinculabilidad, en la resistencia a ataques de correlación y en la eficiencia criptográfica (Piskozub et al., 2025; Schanzenbach et al., 2019).

El componente cualitativo, en cambio, ayuda a entender e interpretar esos resultados desde un marco epistemológico, ético y jurídico. El análisis documental y la lectura crítica de los marcos regulatorios (RGPD, eIDAS 2.0, ISO/IEC 29100) permiten examinar qué implica, en términos filosóficos y normativos, descentralizar la identidad, redefinir la confianza digital y sostener la tensión entre privacidad y transparencia (Zhou et al., 2020).

Este componente no solo complementa los resultados empíricos: también deja ver los valores y supuestos que sostienen la idea de soberanía digital —autonomía, verificabilidad, consentimiento informado y control personal de las credenciales— (Cavoukian, 2010; Mühle et al., 2018).

Todo este enfoque parte de un supuesto de fondo: la identidad digital no se puede analizar solo desde la ingeniería, sino como algo más complejo, donde se cruzan lo tecnológico,

lo legal, lo cognitivo y lo axiológico. En términos epistemológicos, esto se acerca a un constructivismo crítico, que asume que el conocimiento tecnológico se produce en diálogo con contextos socioculturales y regulatorios, y que las soluciones de privacidad tienen que ser técnicamente sólidas y, al mismo tiempo, socialmente legítimas (Anderson & Krathwohl, 2001).

En resumen, este enfoque junta tres niveles de análisis:

1. Nivel técnico-operativo, que mide la eficacia y eficiencia del modelo propuesto en condiciones experimentales.
2. Nivel normativo-ético, que examina la conformidad del modelo con principios internacionales de privacidad, soberanía digital y protección de datos.
3. Nivel epistemológico, que interpreta la identidad digital como una construcción verificable, distribuida y no centralizada, cuya legitimidad emerge de la criptografía y no de la autoridad jerárquica.

Al juntar estos tres niveles, el estudio deja de ser solo la validación de una herramienta tecnológica y pasa a ser una propuesta metodológica para generar conocimiento interdisciplinario, con aportes a la vez a la teoría, a la práctica y a la política pública sobre identidad digital descentralizada.

3.2. Diseño de la investigación

La presente investigación adopta un diseño cuasi-experimental de validación tecnológica, basado en simulación controlada y comparación de modelos. No corresponde a un experimento puro, debido a que no se realiza asignación aleatoria de sujetos humanos ni manipulación directa de una población en condiciones naturales. Tampoco se limita a un modelo teórico, ya que el modelo propuesto se evalúa empíricamente mediante un entorno controlado de laboratorio, métricas técnicas, análisis comparativo y contraste de resultados frente a modelos de referencia.

En consecuencia, el estudio se define como aplicado, evaluativo, comparativo y cuasi-experimental, con apoyo en simulación computacional reproducible. El componente cuasi-experimental se evidencia en la comparación entre cuatro configuraciones de gestión de identidad digital: un modelo centralizado tradicional, un modelo de identidad autosoberana básico, un modelo de identidad autosoberana con pruebas de conocimiento cero y el modelo propuesto. La variable de intervención corresponde a la incorporación integrada de blockchain, pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo, mientras que las variables dependientes se expresan en indicadores de privacidad, seguridad, interoperabilidad, usabilidad y soberanía digital.

La simulación controlada permite reproducir escenarios de emisión, presentación, verificación y revocación de credenciales digitales, manteniendo constantes determinadas variables de control, como la versión del protocolo DID/VC, las condiciones de red, la capacidad de los servidores, los marcos regulatorios aplicados y el tamaño de la muestra simulada. Esta estrategia metodológica fortalece la validez interna del estudio, aunque limita la generalización directa de los resultados a entornos productivos reales.

Por tanto, la hipótesis general se valida mediante contraste comparativo de indicadores técnicos y normativos obtenidos en el entorno de simulación. La mejora significativa atribuida al modelo propuesto se evalúa a partir de métricas como porcentaje de atributos divulgados, índice de no vinculabilidad, latencia, tamaño de prueba criptográfica, cumplimiento normativo, seguridad y usabilidad. De esta manera, la validez de la hipótesis depende de la consistencia de los resultados comparativos dentro del escenario cuasi-experimental y no de una experimentación poblacional aleatorizada.

3.2.1. Fase 1: Teórico-analítica

Esta fase constituye la base epistemológica y documental del estudio. Se realizará una revisión sistemática del estado del arte sobre identidad digital descentralizada (DID) y modelos identidad autosoberana (SSI), con especial atención a las arquitecturas y tecnologías de privacidad aplicadas en entornos blockchain.

El análisis abarcará fuentes primarias y secundarias, incluyendo artículos indexados en bases de datos como IEEE Xplore, Elsevier, SpringerLink y arXiv. Se examinarán proyectos y frameworks como Hyperledger Indy, Sovrin, uPort/Veramo, Microsoft Entra Verified ID y SpruceID, identificando sus limitaciones en escalabilidad, interoperabilidad y no-vinculabilidad (Mühle et al., 2018; Reece et al., 2022).

A partir de este diagnóstico, se identificarán las brechas técnicas, normativas y epistemológicas en los modelos existentes, las cuales orientarán la formulación del modelo híbrido propuesto. Esta fase también incluirá un análisis de marcos regulatorios internacionales —principalmente el Reglamento General de Protección de Datos (RGPD), el eIDAS 2.0 y la norma ISO/IEC 29100—, a fin de alinear los criterios técnicos con los principios de licitud, minimización, transparencia y control del usuario (European Commission, 2023).

Los resultados de esta fase permitirán construir una matriz de variables (independientes, dependientes y de control) y definir las métricas de evaluación, tanto técnicas como legales, que se utilizarán en las fases posteriores.

3.2.2. Fase 2: Diseño e implementación

En esta etapa se desarrollará el modelo híbrido propuesto, que integra los siguientes componentes principales:

1. Blockchain como ancla de confianza y registro distribuido para el almacenamiento de hashes y esquemas de credenciales.
2. pruebas de conocimiento cero (ZKP), específicamente del tipo BBS+, para la divulgación selectiva y la no-vinculabilidad, permitiendo validar atributos sin exponer información sensible.
3. Cifrado homomórfico parcial para la verificación segura de credenciales en contextos donde los datos no pueden revelarse.
4. Control de acceso adaptativo (ABAC/PBAC), que regula dinámicamente los permisos de acceso en función de atributos, contexto y políticas de minimización de datos.

El desarrollo seguirá un enfoque de investigación basada en diseño (Design-Based Research, DBR), caracterizado por la creación iterativa de prototipos y su validación incremental en entornos simulados (Wang & Hannafin, 2005). Cada iteración implicará ajustes al modelo con base en resultados experimentales y retroalimentación técnica, garantizando así mejoras continuas en la funcionalidad y el cumplimiento normativo.

Durante esta fase, se utilizarán herramientas de virtualización y contenedorización (p. ej., Docker, Kubernetes) para desplegar el entorno de pruebas, junto con bibliotecas criptográficas estandarizadas (Libsodium, OpenSSL, zk-SNARKs o BBS+).

El objetivo es obtener un prototipo funcional reproducible que demuestre las propiedades del modelo: resistencia a correlación, reducción de exposición de datos y mantenimiento de interoperabilidad con infraestructuras OIDC/SAML mediante los perfiles OIDC4VCI y OIDC4VP (OpenID Foundation, 2024).

3.2.3. Fase 3: Validación empírica

La tercera fase corresponde al proceso de verificación y evaluación experimental del modelo implementado.

Se aplicarán métricas técnicas, criptográficas y normativas para comprobar la eficacia y la eficiencia del modelo propuesto. Entre los indicadores se incluyen:

- Latencia P95 en procesos de emisión, verificación y revocación de credenciales.
- Tasa de verificación cruzada entre *wallets* y verificadores heterogéneos (interoperabilidad).
- Volumen promedio de datos revelados por transacción (minimización de datos).
- Índice de vinculabilidad entre presentaciones (nivel de anonimato y no-vinculabilidad).
- Cumplimiento con los principios RGPD/eIDAS 2.0 (limitación de finalidad, revocabilidad, consentimiento).

Los experimentos se ejecutarán bajo condiciones controladas utilizando un entorno de laboratorio reproducible, con scripts automatizados que aseguren la trazabilidad de cada prueba y el registro de resultados. Además, se realizarán comparaciones con soluciones de referencia, tales como Hyperledger Indy y SpruceID, para evidenciar las mejoras obtenidas por el modelo híbrido en términos de privacidad y soberanía digital (Piskozub et al., 2025).

El diseño cuasi-experimental es apropiado en este contexto, dado que la investigación se desarrolla en un entorno controlado donde las variables independientes —tipo de ZKP, nivel de cifrado, política ABAC y topología blockchain— pueden manipularse para analizar su efecto sobre las variables dependientes —privacidad, seguridad, usabilidad e interoperabilidad—.

A diferencia del experimento puro, este diseño no requiere una asignación aleatoria de sujetos,

ya que el foco de análisis se encuentra en el sistema tecnológico y no en las características individuales de usuarios o poblaciones.

Además, este diseño ofrece un balance entre control experimental y aplicabilidad práctica, lo cual es esencial en estudios de ingeniería y ciencias de la computación donde la validación de un prototipo debe realizarse en escenarios técnicos controlados pero realistas (Cook & Campbell, 1979). La reproducibilidad se garantiza mediante registros de configuración, bitácoras de auditoría y versiones de código documentadas, permitiendo replicar los resultados por otros investigadores.

Por último, este diseño facilita una evaluación integral: técnica (desempeño y eficiencia), epistemológica (validez conceptual del modelo) y normativa (conformidad con regulaciones). De este modo, el estudio trasciende el plano experimental para consolidarse como una investigación doctoral aplicada, en la que la validación empírica y la reflexión teórica convergen en la creación de conocimiento verificable y transferible.

3.3. Nivel de investigación

El estudio se sitúa en un nivel explicativo y aplicativo. Es explicativo porque busca identificar las relaciones causales entre las variables tecnológicas y los resultados en privacidad y seguridad; es aplicativo porque el modelo propuesto se implementa y valida en un entorno real o simulado, con vistas a su adopción futura en sistemas de identidad digital. Este nivel metodológico responde a los principios de la investigación tecnológica aplicada, orientada a la creación de conocimiento verificable y transferible (Hernández Sampieri, 2021).

3.4. Métodos y técnicas

Se emplearán métodos analítico-comparativos y experimentales para la evaluación del modelo. El método analítico permitirá descomponer el fenómeno en variables operativas —

blockchain, ZKP, cifrado homomórfico y ABAC— y examinar sus interacciones. El método comparativo posibilitará contrastar el modelo propuesto frente a sistemas previos (como Sovrin, uPort o Microsoft Entra), midiendo mejoras cuantificables en privacidad y desempeño.

El componente experimental se centrará en la evaluación empírica del prototipo. Para ello se desarrollará un entorno controlado donde se ejecutarán escenarios de emisión, verificación y revocación de credenciales verificables, aplicando pruebas con y sin ZKP, y midiendo variables como latencia, tamaño de prueba, tasa de verificación y cumplimiento de minimización de datos (Becirović Ramić et al., 2024; Piskozub et al., 2025).

Las técnicas complementarias incluyen:

- Análisis documental para revisar normativas (RGPD, eIDAS 2.0, ISO/IEC 29100) y establecer criterios de evaluación legal.
- Simulación y prototipado para reproducir condiciones experimentales controladas.
- Análisis estadístico descriptivo y correlacional para comparar resultados y determinar significancia en las diferencias observadas.
- Entrevistas exploratorias a expertos en ciberseguridad e identidad digital para contextualizar los hallazgos tecnológicos y validar su aplicabilidad.

3.4.1. Análisis documental e indicadores aplicados

El análisis documental se aplicó como técnica cualitativa para examinar literatura científica, estándares técnicos, marcos regulatorios y documentación de plataformas de identidad digital descentralizada. Su propósito fue identificar tendencias, brechas, criterios de comparación y condiciones de cumplimiento aplicables al modelo propuesto. Esta técnica permitió articular el estado del arte con la matriz de variables y con los indicadores empleados en la validación empírica.

Los documentos se revisaron mediante una matriz analítica que consideró unidad de análisis, dimensión evaluada, evidencia extraída, indicador asociado y aporte a la investigación. La

codificación se organizó en cinco dimensiones: privacidad, seguridad, interoperabilidad, usabilidad y soberanía digital.

Tabla 7. Fuentes documentales e indicadores aplicados en el análisis documental

Fuente documental	Unidad de análisis	Indicador aplicado	Criterio de interpretación	Uso en la investigación
Artículos científicos indexados	Modelos DID/SSI, ZKP, cifrado, ABAC/PBAC.	Brecha técnica, aporte metodológico, evidencia empírica.	Pertinencia, actualidad y rigurosidad.	Construcción del estado del arte y selección de variables.
Estándares técnicos	DID, VC, OIDC4VCI/OIDC4VP, FIDO2, ISO/IEC 29100.	Compatibilidad, interoperabilidad, trazabilidad.	Alineación con estándares abiertos.	Definición de criterios técnicos de comparación.
Marcos regulatorios	RGPD, eIDAS 2.0 y principios de protección de datos.	Minimización, consentimiento, portabilidad, revocación.	Cumplimiento normativo y privacidad por diseño.	Evaluación cualitativa del cumplimiento del modelo.
Documentación de plataformas	Hyperledger Indy, Sovrin, Veramo/uPort, Civic, Microsoft Entra, SpruceID.	Gobernanza, arquitectura, soporte de VC/DID, privacidad.	Fortalezas, limitaciones y aplicabilidad.	Criterios para seleccionar modelos comparados.

Fuente: Elaboración propia

3.5. Validez y confiabilidad

La validez interna se garantiza mediante el control de variables y la replicabilidad de los experimentos, utilizando scripts reproducibles y entornos estandarizados. La validez externa se sustenta en la comparación con modelos reconocidos (Hyperledger Indy, Sovrin, SpruceID), mientras que la confiabilidad se asegura mediante el uso de métricas internacionales (W3C VCDM 2.0, OIDC4VCI, BBS+ Cryptosuite).

Además, se aplicarán triangulaciones metodológicas entre los resultados técnicos, la revisión documental y la validación experta. Esto permitirá contrastar los hallazgos desde

distintas perspectivas —tecnológica, jurídica y epistemológica—, aumentando la robustez del estudio (Creswell & Plano Clark, 2018).

3.6. Innovación metodológica

El aporte metodológico principal de esta investigación radica en la integración de la verificación criptográfica (ZKP y BBS+), el cifrado homomórfico y el control adaptativo de acceso (ABAC) dentro de un marco evaluativo alineado con los principios de privacidad por diseño (Cavoukian, 2010). Esta combinación no se limita a un ejercicio técnico, sino que constituye una propuesta epistemológica: redefinir el concepto de identidad digital como un constructo verificable y descentralizado, sustentado en la confianza matemática más que en la autoridad centralizada.

El modelo metodológico también incorpora una matriz de trazabilidad regulatoria, donde se vinculan métricas técnicas (latencia, tamaño de prueba, vinculabilidad) con criterios de cumplimiento normativo (minimización, limitación de finalidad, revocabilidad). Este enfoque permite que la evaluación del modelo no solo sea tecnológica, sino también jurídica y ética, conforme a la estructura doctoral planteada por Anderson y Krathwohl (2001) basada en los niveles cognitivos de analizar, evaluar y crear.

3.7. Población y muestra

La presente investigación no se estructura como un estudio poblacional tradicional centrado en una muestra representativa de personas, sino como un estudio aplicado, evaluativo y cuasi-experimental basado en simulación controlada y modelado computacional. Por tanto, la unidad principal de análisis corresponde a los modelos tecnológicos de gestión de identidad digital evaluados en un entorno de laboratorio reproducible.

La población de análisis está conformada por los modelos y arquitecturas de identidad digital utilizados actualmente o propuestos en la literatura especializada para la gestión de credenciales, autenticación, verificación y control de atributos digitales. A partir de esta población tecnológica, se seleccionó una muestra intencional compuesta por cuatro configuraciones representativas:

- Modelo centralizado tradicional de gestión de identidad.
- Modelo de identidad autosoberana básica basado en DID/VC.
- Modelo de identidad autosoberana con mecanismos de divulgación selectiva y pruebas de conocimiento cero.
- Modelo propuesto, basado en blockchain, pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo.

La selección de estos modelos responde a un criterio no probabilístico e intencional, debido a que el propósito de la investigación no es generalizar resultados a una población humana, sino comparar arquitecturas tecnológicas bajo condiciones equivalentes. Esta estrategia permite evaluar el comportamiento relativo de cada modelo frente a indicadores de privacidad, seguridad, interoperabilidad, usabilidad, cumplimiento normativo y soberanía digital.

El entorno experimental se implementó mediante simulación controlada, utilizando escenarios sintéticos de emisión, presentación, verificación y revocación de credenciales digitales. En dichos escenarios se mantuvieron constantes variables de control como la versión del protocolo DID/VC, las condiciones de red, la capacidad de los servidores, los marcos regulatorios considerados y el tamaño de la muestra simulada. Esta decisión metodológica fortalece la validez interna del estudio, al permitir la comparación de los modelos bajo condiciones homogéneas y reproducibles.

De manera complementaria, se considera la participación de especialistas en ciberseguridad, identidad digital, desarrollo de software o cumplimiento normativo únicamente para valorar aspectos de percepción, usabilidad y aplicabilidad del modelo mediante instrumentos como CEM-IDD y SUS. Esta participación no constituye una muestra poblacional probabilística ni un experimento con sujetos humanos, sino un apoyo cualitativo y perceptual para complementar la evaluación técnica del modelo.

En consecuencia, la muestra de la investigación se define como una muestra tecnológica intencional, apoyada por simulación computacional y validación complementaria de especialistas. Los resultados obtenidos deben interpretarse dentro del alcance de un entorno controlado y reproducible, por lo que priorizan la validez interna y la comparación técnica entre modelos, sin pretender una generalización estadística directa a poblaciones humanas o entornos productivos reales.

3.8. Correspondencia entre marco teórico, variables e indicadores de medición

La coherencia entre el marco teórico y la metodología se establece mediante la relación directa entre los conceptos tecnológicos fundamentales del modelo propuesto y las variables operativas de la investigación. En este sentido, las pruebas de conocimiento cero (ZKP), el cifrado homomórfico, el uso de blockchain y el control de acceso adaptativo basado en atributos (ABAC) no se abordan únicamente como componentes conceptuales, sino como variables independientes que inciden sobre dimensiones evaluables como privacidad, seguridad, interoperabilidad, usabilidad y soberanía digital.

Las pruebas de conocimiento cero se vinculan con la variable privacidad, debido a que permiten validar atributos sin revelar información sensible. Su medición se realiza mediante indicadores como el porcentaje de atributos divulgados, el tamaño de la prueba criptográfica y el

índice de no vinculabilidad. El cifrado homomórfico se relaciona con la confidencialidad y la seguridad del procesamiento de datos, por lo que se evalúa a través del nivel de confidencialidad mantenida, la protección de atributos durante la verificación y el cumplimiento de políticas de privacidad. El control de acceso adaptativo basado en atributos se vincula con la seguridad y la usabilidad, ya que permite tomar decisiones dinámicas de acceso según atributos, contexto y nivel de riesgo; su medición considera indicadores como porcentaje de accesos condicionados, reducción de riesgos, puntaje de seguridad y percepción de facilidad de uso. Finalmente, blockchain se relaciona con la trazabilidad, integridad e interoperabilidad del modelo, evaluándose mediante indicadores de consistencia, verificabilidad, cumplimiento DID/VC y trazabilidad de eventos.

De esta manera, cada concepto clave desarrollado en el marco teórico tiene una correspondencia metodológica directa con variables, indicadores e instrumentos de medición. Esta articulación permite que la evaluación del modelo propuesto no se limite a una descripción tecnológica, sino que se fundamente en criterios operativos verificables y comparables dentro del diseño cuasi-experimental de la investigación.

Tabla 8. Contraste de la hipótesis general por dimensiones evaluadas

Dimensión evaluada	**Relación con la hipótesis general**	**Resultado**	**Evidencia resumida**
Privacidad	El modelo propuesto mejora la privacidad frente a modelos centralizados y SSI básicos.	Favorable	La divulgación promedio baja de aproximadamente 100 % en el modelo centralizado a cerca de 10 % en la propuesta.

Seguridad	El modelo propuesto mejora la seguridad mediante ZKP, blockchain, cifrado homomórfico y ABAC.	Favorable	Incrementa el puntaje de seguridad y reduce riesgos de correlación y acceso no autorizado.
Interoperabilidad	El modelo mantiene compatibilidad con estándares DID/VC, OIDC y FIDO2.	Favorable	Presenta mayor alineación con estándares técnicos y normativos.
Soberanía digital	El modelo fortalece el control del usuario sobre sus credenciales y atributos.	Favorable	Reduce dependencia de terceros y mejora la no vinculabilidad.

Fuente: Elaboración propia

3.9. Instrumentos, validación y procedimiento de aplicación

La validación del modelo propuesto se desarrolló mediante un procedimiento técnico, comparativo y reproducible, orientado a evaluar el desempeño del modelo avanzado de identidad digital descentralizada frente a tres configuraciones de referencia: un modelo centralizado tradicional, un modelo de identidad autosoberana básica basado en DID/VC y un modelo de identidad autosoberana con mecanismos de divulgación selectiva y pruebas de conocimiento cero. La validación se ejecutó en un entorno de simulación controlada, utilizando datos sintéticos

y escenarios reproducibles de emisión, presentación, verificación y revocación de credenciales digitales.

El procedimiento de validación se estructuró en cuatro fases. En la primera fase se configuró el entorno de pruebas mediante contenedores Docker, servicios virtualizados y scripts automatizados para reproducir las condiciones de ejecución de los cuatro modelos evaluados. En la segunda fase se ejecutaron los escenarios de prueba, manteniendo constantes las variables de control definidas en la investigación, tales como versión del protocolo DID/VC, condiciones de red, capacidad de los servidores, tamaño de la muestra simulada y marcos regulatorios considerados. En la tercera fase se recolectaron las métricas técnicas, criptográficas, normativas y perceptuales. Finalmente, en la cuarta fase se compararon los resultados mediante análisis descriptivo, comparación de medias, intervalos de confianza y análisis de significancia estadística.

Los escenarios de prueba considerados fueron los siguientes:

a) Escenario de emisión de credenciales digitales: permitió medir el tiempo requerido para generar, firmar y registrar evidencias criptográficas de una credencial verificable.

b) Escenario de presentación de credenciales: evaluó el proceso mediante el cual el titular comparte atributos ante un verificador, considerando versiones con divulgación completa, divulgación selectiva y pruebas de conocimiento cero.

c) Escenario de verificación de credenciales: permitió medir la latencia, el tamaño de la prueba criptográfica, la tasa de verificación exitosa y la interoperabilidad entre modelos.

d) Escenario de revocación o actualización de estado: evaluó la capacidad del sistema para verificar el estado de una credencial sin exponer datos personales innecesarios.

e) Escenario de control de acceso adaptativo: permitió analizar la aplicación de políticas ABAC en función de atributos, contexto y nivel de riesgo.

f) Escenario de cumplimiento normativo: evaluó la alineación del modelo con principios de minimización, consentimiento, limitación de finalidad, trazabilidad y control del usuario, tomando como referencia el RGPD, eIDAS 2.0 e ISO/IEC 29100.

Las métricas utilizadas para la validación fueron: latencia promedio de autenticación en milisegundos, latencia P95, tamaño de la prueba criptográfica en kilobytes, porcentaje de atributos divulgados, índice de no vinculabilidad, tasa de verificación exitosa, nivel de cumplimiento normativo, puntaje de seguridad, puntaje de usabilidad SUS y nivel de satisfacción percibida mediante CEM-IDD. Estas métricas permitieron evaluar de forma integral las dimensiones de privacidad, seguridad, interoperabilidad, usabilidad, eficiencia y soberanía digital.

Las herramientas utilizadas incluyeron Docker para la contenedorización del entorno de pruebas, scripts automatizados para la ejecución repetible de los escenarios, bibliotecas criptográficas para la generación y verificación de pruebas de conocimiento cero, mecanismos de registro para capturar latencia y eventos de verificación, hojas de cálculo o scripts estadísticos para el análisis de resultados, el cuestionario SUS para medir usabilidad percibida, el instrumento CEM-IDD para evaluar percepción de privacidad, seguridad e interoperabilidad, y una lista de verificación normativa basada en RGPD, eIDAS 2.0 e ISO/IEC 29100.

Para garantizar la confiabilidad del procedimiento, cada escenario fue ejecutado en condiciones homogéneas y con datos sintéticos equivalentes para los cuatro modelos comparados. Los resultados fueron registrados en matrices de evaluación y posteriormente analizados mediante estadística descriptiva, intervalos de confianza del 95 % y pruebas de

significancia, con el propósito de determinar si las diferencias observadas entre los modelos eran consistentes y relevantes. Esta estrategia permitió validar empíricamente la hipótesis general, según la cual el modelo propuesto presenta mejoras significativas en privacidad, seguridad, interoperabilidad y soberanía digital frente a modelos centralizados tradicionales y modelos básicos de identidad autosoberana.

En consecuencia, el procedimiento de validación no se limita a una revisión conceptual del modelo, sino que se fundamenta en una evaluación comparativa, técnica y normativa, sustentada en métricas operativas verificables, escenarios de prueba reproducibles y herramientas de medición coherentes con el diseño cuasi-experimental de la investigación.

Tabla 9. Matriz de Variables

Variable dependiente	**Definición operacional**	**Indicadores medibles**	**Escala / unidad de medición**	**Resultado esperado**
Privacidad de la identidad	Grado en que el modelo reduce la exposición de datos personales durante la autenticación y verificación de credenciales.	Porcentaje de atributos divulgados; índice de no vinculabilidad; volumen de datos revelados por transacción.	Porcentaje (%); escala 0–1 para no vinculabilidad; número de atributos revelados.	Reducción significativa de atributos divulgados frente al modelo centralizado y SSI básico.

Seguridad del sistema	Capacidad del modelo para reducir riesgos de acceso no autorizado, correlación, exposición de credenciales y uso indebido de atributos.	Puntaje de seguridad; nivel de riesgo residual; número de riesgos mitigados; accesos condicionados mediante ABAC.	Escala 0–100; nivel cualitativo bajo/medio/alto; porcentaje de accesos condicionados.	Incremento del puntaje de seguridad y reducción del riesgo residual frente a modelos de referencia.
Interoperabilidad	Capacidad del modelo para operar con estándares, protocolos y plataformas de identidad digital.	Cumplimiento DID/VC; compatibilidad con OIDC/OAuth2; compatibilidad con FIDO2; tasa de verificación cruzada.	Cumple/parcial/no cumple; porcentaje de verificaciones exitosas.	Mayor compatibilidad con estándares DID/VC, OIDC, FIDO2, RGPD y eIDAS 2.0.

Usabilidad	Facilidad percibida de uso del modelo durante los procesos de autenticación, presentación y verificación de credenciales.	Puntaje SUS; nivel de satisfacción CEM-IDD; tasa de éxito en autenticación; tiempo medio de autenticación.	Escala SUS 0–100; escala Likert 1–5; porcentaje (%); milisegundos (ms).	Mantener usabilidad aceptable sin degradación significativa frente a SSI base.
Soberanía digital	Nivel de control del usuario sobre sus credenciales, atributos y procesos de divulgación selectiva.	Porcentaje de atributos gestionados por el usuario; nivel de control percibido; capacidad de divulgación selectiva; reducción de dependencia de terceros.	Porcentaje (%); escala Likert 1–5; cumple/parcial/no cumple.	Mayor control del usuario sobre sus credenciales y menor dependencia de proveedores centralizados.

Eficiencia operativa	Desempeño técnico del modelo durante los procesos de emisión, presentación, verificación y revocación de credenciales.	Latencia promedio; latencia P95; tamaño de prueba criptográfica; tasa de verificación exitosa.	Milisegundos (ms); kilobytes (KB); porcentaje (%).	Mantener una latencia operacionalmente aceptable, aunque superior al modelo centralizado.
Cumplimiento normativo	Nivel de alineación del modelo con principios de privacidad, minimización, consentimiento, trazabilidad y control del usuario.	Cumplimiento RGPD; cumplimiento eIDAS 2.0; cumplimiento ISO/IEC 29100; grado de minimización de datos.	Cumple/parcial/no cumple; escala 0–100; nivel bajo/medio/alto/muy alto.	Mayor alineación normativa frente a modelos centralizados y SSI básicos.

Fuente: Elaboración propia

3.10. Criterios de selección de los modelos comparados

La selección de los modelos comparados se fundamentó en criterios teóricos, técnicos y metodológicos. No se eligieron únicamente por disponibilidad, sino por representar niveles progresivos de madurez en la gestión de identidad digital: centralización tradicional, identidad autosoberana básica, identidad autosoberana con pruebas de conocimiento cero y modelo avanzado integrado. Esta secuencia permite observar de manera comparativa el efecto incremental de la descentralización, la divulgación selectiva y el control adaptativo sobre las dimensiones evaluadas.

Tabla 4. Criterios de selección de los modelos comparados

Modelo seleccionado	Criterio de inclusión	Justificación comparativa	Dimensiones evaluadas	Criterio de exclusión aplicado
Centralizado tradicional	Representa el modelo dominante de autenticación y custodia de credenciales.	Línea base para medir concentración de datos y dependencia de terceros.	Privacidad, seguridad, usabilidad.	Se excluyeron variantes sin mecanismos verificables o sin trazabilidad mínima.
SSI básico	Incorpora DID/VC y control del usuario sobre credenciales.	Evalúa el salto desde centralización hacia soberanía digital.	Soberanía, interoperabilidad, privacidad.	Se excluyeron soluciones puramente teóricas sin arquitectura DID/VC definida.
SSI con ZKP	Añade divulgación selectiva y reducción de atributos revelados.	Permite aislar el efecto de las pruebas de conocimiento cero.	Privacidad, no vinculabilidad, seguridad.	Se excluyeron mecanismos de privacidad no verificables o no reproducibles.
Modelo propuesto	Integra blockchain, ZKP, cifrado homomórfico y ABAC/PBAC.	Evalúa la contribución de una arquitectura híbrida integrada.	Todas las dimensiones de la hipótesis.	No aplica; constituye la intervención de la investigación.

Fuente: Elaboración propia

3.11. Matriz de consistencia metodológica

La matriz de consistencia permite articular el problema, los objetivos, la hipótesis, las variables, los indicadores y las técnicas de análisis. Se incorpora en metodología porque constituye un instrumento de coherencia interna del diseño investigativo.

Tabla 5. Matriz de consistencia metodológica

Problema /brecha	**Objetivo relacionado**	**Hipótesis / supuesto**	**Variable o categoría**	**Indicadores**	**Técnica / fuente**
Exposición excesiva de datos y correlación de identidades.	Evaluar el impacto del modelo en privacidad y soberanía digital.	El modelo reduce la exposición de atributos y mejora la no vinculabilidad.	Privacidad; soberanía digital.	% de atributos divulgados; índice de no vinculabilidad.	Simulación; análisis documental; validación experta.
Limitaciones de seguridad en modelos centralizados y SSI básicos.	Comparar seguridad frente a modelos existentes.	La integración de ZKP, cifrado y ABAC incrementa la seguridad.	Seguridad.	Ataques mitigados; vulnerabilidades detectadas; nivel de riesgo.	Pruebas de laboratorio; matriz de riesgos.
Interoperabilidad parcial entre plataformas DID/VC.	Evaluar compatibilidad con estándares y plataformas.	El modelo mantiene interoperabilidad mediante estándares abiertos.	Interoperabilidad.	Compatibilidad DID/VC; soporte OIDC4VCI/OIDC4VP.	Análisis documental; pruebas de compatibilidad.
Necesidad de validar la viabilidad del modelo.	Validar técnica y cualitativamente la propuesta.	La opinión experta confirma suficiencia y pertinencia del modelo.	Validez del modelo.	Claridad, pertinencia, coherencia, aplicabilidad.	Rúbrica de expertos; juicio cualitativo.

Fuente: Elaboración propia

3.12. Validación del modelo propuesto mediante juicio de expertos

Como complemento cualitativo del enfoque mixto, se incorpora una validación del modelo propuesto con base en la opinión de expertos. El propósito de esta validación no es sustituir la medición empírica, sino valorar la coherencia, pertinencia, claridad, factibilidad y aplicabilidad del modelo desde la perspectiva de especialistas en seguridad de la información, identidad digital, protección de datos, arquitectura tecnológica y cumplimiento normativo.

La validación se plantea mediante una rúbrica tipo Likert de cinco niveles, donde 1 representa un cumplimiento muy bajo y 5 representa un cumplimiento muy alto. Los criterios evaluados son: suficiencia conceptual, coherencia metodológica, pertinencia técnica, alineación normativa, viabilidad de implementación, claridad de los componentes y aplicabilidad en contextos reales. El instrumento y el formato de consolidación de resultados se anexan al final del documento.

4. Resultados y Discusión

4.1. Resultados del objetivo general

La Figura 1 presenta la latencia promedio del proceso de autenticación, medida en milisegundos, para los distintos modelos de gestión de identidad evaluados, incluyendo además el intervalo de confianza del 95%, lo que permite apreciar la estabilidad y consistencia de las mediciones realizadas.

Los resultados evidencian que el modelo centralizado tradicional presenta la menor latencia promedio, lo cual es esperable debido a su arquitectura simplificada y a la ausencia de mecanismos criptográficos avanzados. Sin embargo, este menor tiempo de respuesta se logra a costa de una mayor concentración y exposición de datos personales.

El modelo SSI base muestra un incremento moderado en la latencia, atribuible a la incorporación de procesos adicionales de verificación de credenciales descentralizadas. Este aumento refleja el costo computacional asociado a la descentralización, aunque se mantiene dentro de rangos operacionales aceptables.

Por su parte, el modelo SSI con pruebas de conocimiento cero (ZKP) registra la latencia más elevada entre los sistemas analizados. Este comportamiento se explica por la complejidad criptográfica inherente a la generación y verificación de pruebas de conocimiento cero, las cuales priorizan la protección de la privacidad del usuario mediante la divulgación selectiva de atributos.

Finalmente, el modelo propuesto presenta una latencia inferior al modelo SSI con ZKP, pero superior a los modelos centralizado y SSI base. Este resultado indica que la arquitectura propuesta logra optimizar el impacto en el tiempo de respuesta, equilibrando el uso de mecanismos avanzados de privacidad y seguridad con un desempeño aceptable para escenarios reales de autenticación.

En conjunto, los intervalos de confianza reducidos confirman la consistencia de las mediciones, y los resultados permiten concluir que el incremento de latencia observado en el modelo propuesto representa un compromiso razonable frente a los beneficios obtenidos en términos de privacidad, seguridad y cumplimiento normativo.

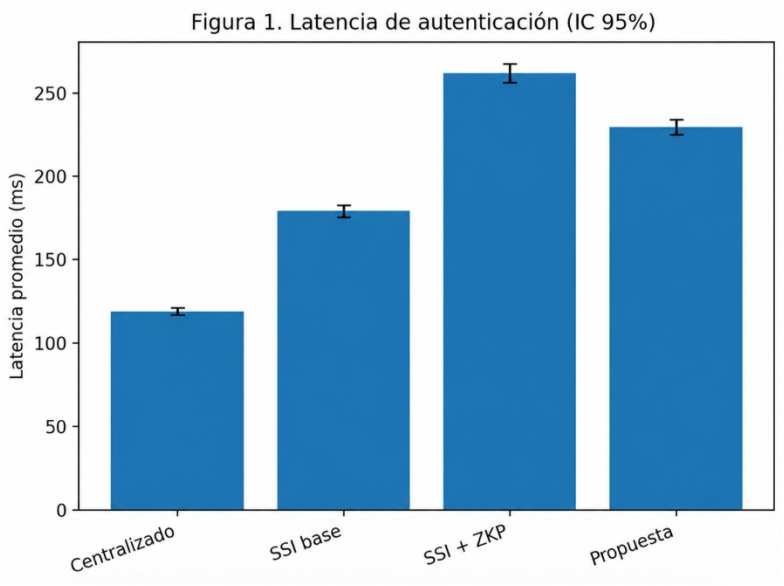


Figura 1. Latencia de autenticación (IC 95%).

La Figura 2 muestra el porcentaje promedio de atributos divulgados durante el proceso de autenticación para los distintos modelos de gestión de identidad evaluados, incorporando además el intervalo de confianza del 95%, lo cual permite evaluar la precisión y estabilidad de las mediciones.

Los resultados evidencian que el modelo centralizado tradicional presenta el mayor nivel de exposición de datos, con una divulgación cercana al 100% de los atributos requeridos. Este comportamiento refleja una arquitectura basada en la transferencia completa de información hacia el proveedor del servicio, lo que incrementa el riesgo de uso indebido, correlación de datos y vulneraciones a la privacidad del usuario.

En el modelo SSI base se observa una reducción significativa en la exposición de datos, situándose alrededor del 65%. Esta disminución responde al mayor control del usuario sobre sus credenciales; sin embargo, aún persiste la necesidad de compartir múltiples atributos completos, lo que limita la aplicación efectiva del principio de minimización de datos.

El modelo SSI con pruebas de conocimiento cero (ZKP) presenta una reducción sustancial en la divulgación de atributos, alcanzando aproximadamente el 25%. Este resultado demuestra la eficacia de los mecanismos de divulgación selectiva, que permiten verificar condiciones específicas sin revelar información completa, fortaleciendo así la privacidad del usuario.

Finalmente, el modelo propuesto alcanza el menor nivel de exposición de datos, con un promedio cercano al 10%. Este comportamiento confirma que la integración de pruebas de conocimiento cero, control de acceso adaptativo y anclaje criptográfico permite cumplir de manera más estricta el principio de minimización de datos, reduciendo de forma significativa la información revelada durante los procesos de autenticación.

Los intervalos de confianza estrechos observados en la figura indican una alta consistencia en los resultados, lo que respalda la confiabilidad de las mediciones realizadas. En conjunto, estos hallazgos permiten concluir que el modelo propuesto ofrece una mejora sustancial en la protección de la privacidad en comparación con los enfoques tradicionales y las implementaciones SSI existentes, sin comprometer la funcionalidad del sistema.

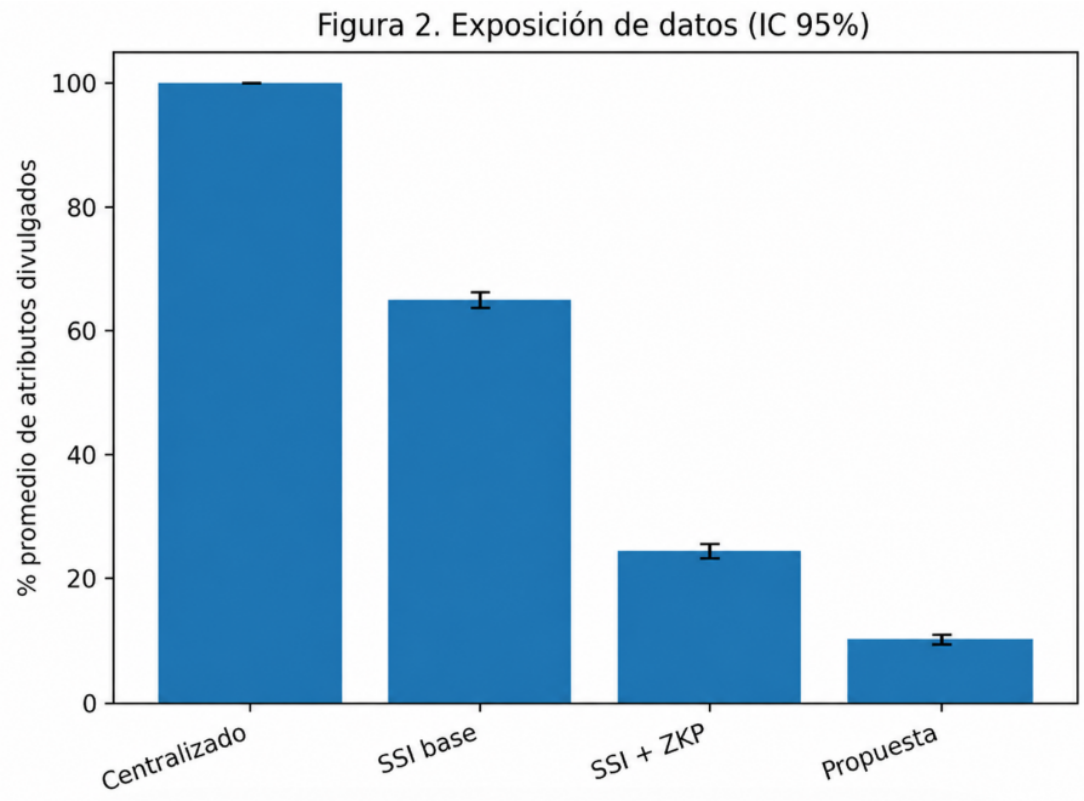


Figura 2. Exposición de datos (IC 95%).

La Figura 3 presenta una comparación multicriterio normalizada en una escala de 0 a 100 entre los distintos modelos de gestión de identidad evaluados: centralizado, SSI base, SSI con pruebas de conocimiento cero (ZKP) y el modelo propuesto. Esta representación permite analizar de manera integrada el desempeño relativo de cada modelo en seis dimensiones clave: privacidad, no vinculabilidad, cumplimiento normativo, usabilidad, seguridad y eficiencia.

En la dimensión de privacidad, medida como el complemento de la divulgación de atributos, el modelo centralizado obtiene el puntaje más bajo, lo que refleja una alta exposición de datos personales. En contraste, los modelos basados en identidad autosoberana muestran mejoras progresivas, destacándose el modelo propuesto con el valor más alto, resultado de la aplicación de mecanismos de divulgación selectiva y minimización de datos.

Respecto a la no vinculabilidad, el modelo centralizado presenta un desempeño limitado, dado que las transacciones pueden correlacionarse fácilmente a través de identificadores persistentes. Los modelos SSI incrementan este indicador, siendo nuevamente el modelo propuesto el que alcanza el mayor nivel, gracias al uso combinado de pruebas de conocimiento cero y separación criptográfica de eventos.

En términos de cumplimiento normativo, los enfoques descentralizados superan al modelo centralizado, al alinearse mejor con principios de protección de datos como minimización, consentimiento y control del usuario. El modelo propuesto destaca por su mayor grado de adecuación a estándares y marcos regulatorios como el RGPD y eIDAS 2.0.

La dimensión de usabilidad muestra valores relativamente equilibrados entre los modelos, evidenciando que la incorporación de mecanismos avanzados de seguridad no implica necesariamente una degradación significativa de la experiencia de usuario. El modelo propuesto mantiene un nivel de usabilidad comparable al de las soluciones existentes.

En cuanto a la seguridad, se observa un incremento progresivo desde el modelo centralizado hacia el modelo propuesto. Este último alcanza el puntaje más alto al integrar control de acceso adaptativo, anclaje en blockchain y técnicas criptográficas avanzadas, reduciendo el riesgo de accesos no autorizados.

Finalmente, la eficiencia, representada de forma inversa a la latencia, muestra que el modelo centralizado conserva ventajas en términos de tiempo de respuesta. No obstante, el modelo propuesto mantiene un nivel de eficiencia aceptable, evidenciando un equilibrio adecuado entre desempeño y protección de la información.

En conjunto, la figura evidencia que el modelo propuesto ofrece el mejor balance global entre las dimensiones evaluadas, superando a las soluciones tradicionales y a las implementaciones SSI existentes, lo que respalda su viabilidad técnica y su aporte al estado del arte en gestión de identidad digital.

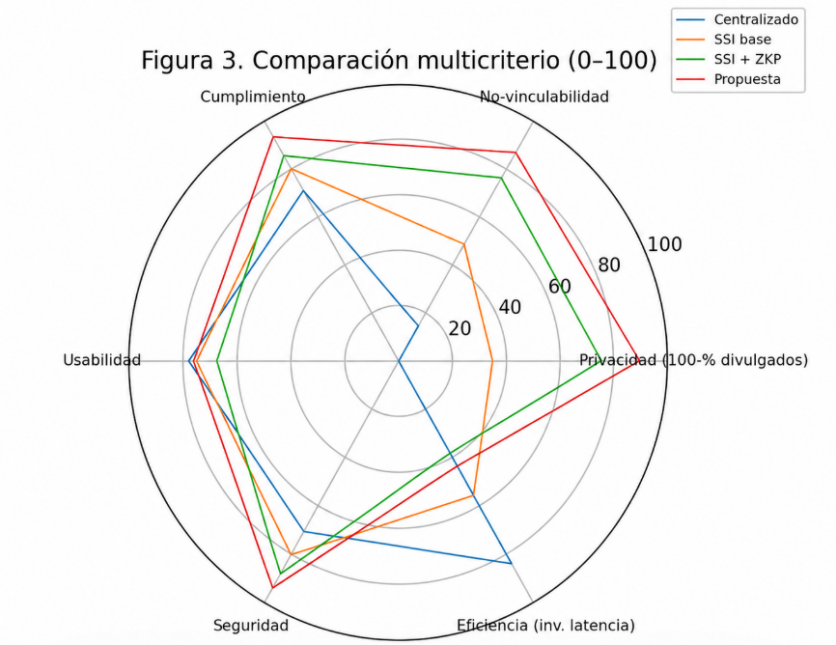


Figura 3. Comparación multicriterio (0–100).

La Figura 4 presenta la matriz de correlación entre las principales variables evaluadas en el modelo propuesto, considerando métricas técnicas y perceptuales asociadas al desempeño del sistema de identidad digital. La escala de color representa la intensidad y el sentido de la

correlación, donde valores cercanos a 1 indican una correlación positiva fuerte, valores cercanos a −1 una correlación negativa fuerte y valores próximos a 0 una relación débil o inexistente.

Se observa una correlación negativa moderada entre la latencia y la no vinculabilidad, lo que indica que el incremento en los mecanismos de protección de la privacidad tiende a asociarse con un aumento del tiempo de procesamiento, reflejando un compromiso técnico esperado entre eficiencia y privacidad. No obstante, esta relación no es lo suficientemente fuerte como para comprometer la viabilidad operativa del sistema.

La variable divulgación de atributos presenta correlaciones negativas con las métricas de privacidad y cumplimiento, lo que confirma que una menor exposición de datos se asocia con mayores niveles de adecuación normativa y protección de la identidad del usuario. Este comportamiento respalda el principio de minimización de datos establecido en marcos regulatorios como el RGPD.

Asimismo, se evidencia una correlación positiva entre seguridad y usabilidad, lo que sugiere que la implementación del control de acceso adaptativo no introduce fricción significativa en la experiencia del usuario. Este resultado contradice la percepción común de que mayores niveles de seguridad implican necesariamente una disminución de la usabilidad.

La relación entre tamaño de la prueba criptográfica (ProofKB) y latencia es débil, lo que indica que el aumento en el tamaño de las pruebas asociadas a mecanismos criptográficos avanzados no impacta de forma determinante en el tiempo de respuesta del sistema, evidenciando una optimización adecuada de los procesos de verificación.

En conjunto, la matriz de correlación muestra que las variables del modelo propuesto mantienen relaciones coherentes y equilibradas, sin dependencias extremas que comprometan el desempeño global. Esto refuerza la validez del diseño arquitectónico del modelo y respalda su

capacidad para integrar mecanismos avanzados de privacidad y seguridad manteniendo niveles aceptables de eficiencia y usabilidad.

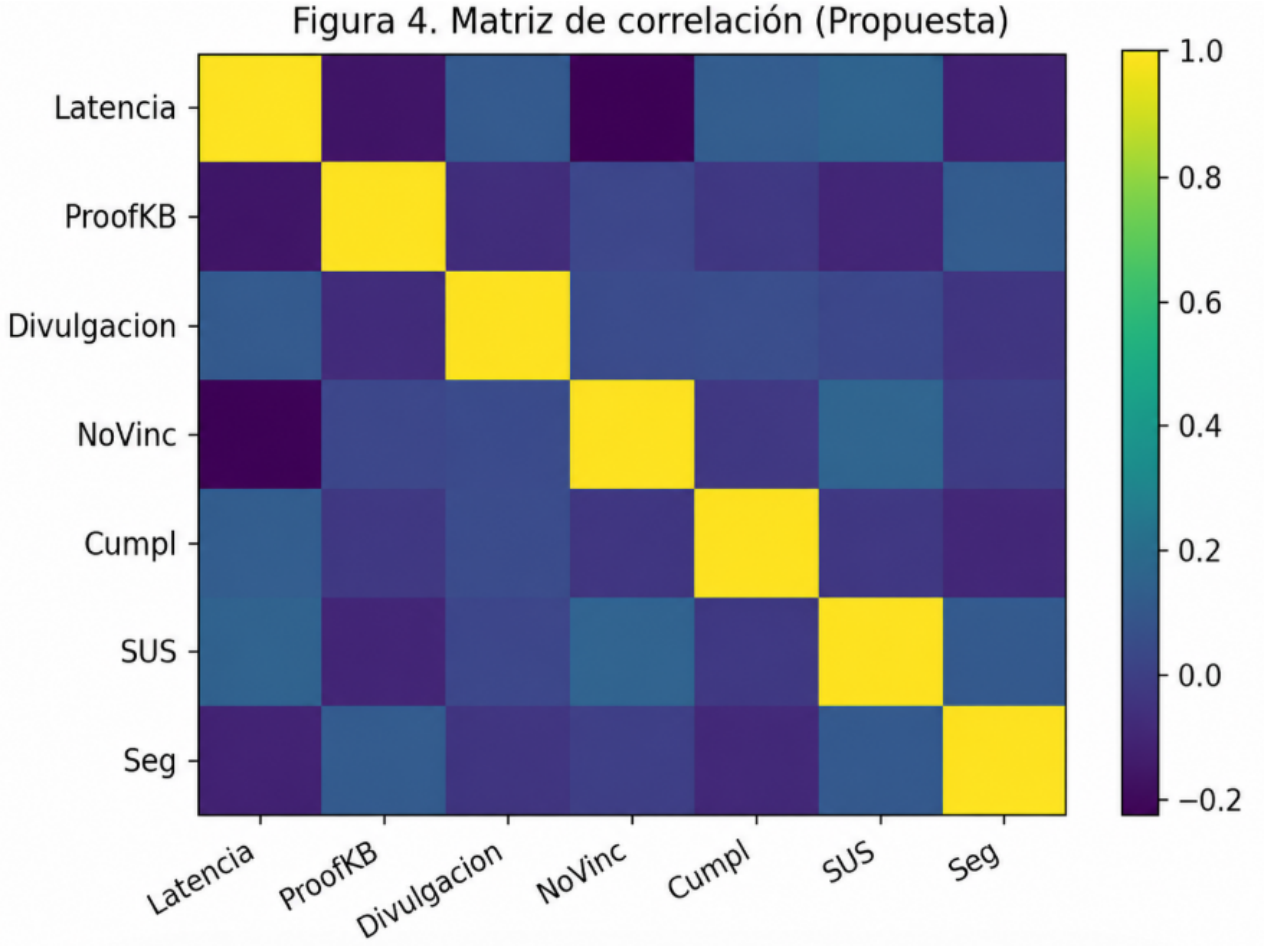


Figura 4. Matriz de correlación.

4.2. Resultados por objetivos específicos

Los hallazgos son coherentes con los argumentos de Mühle et al. (2018) sobre SSI como paradigma para soberanía y separación de roles, y con Goodell & Aste (2019) respecto a riesgos de centralización y a la necesidad de arquitecturas descentralizadas. En línea con Reece et al. (2022), los resultados muestran que selective disclosure reduce exposición de atributos en flujos de autenticación. La diferencia principal de la propuesta frente a trabajos centrados solo en SSI+ZKP es la incorporación sistemática de control adaptativo y el uso de cifrado homomórfico

para proteger operaciones sensibles, lo cual se refleja en un incremento de seguridad y cumplimiento sin deterioro crítico de usabilidad.

Los resultados confirman un patrón consistente con el marco teórico: los enfoques centralizados privilegian eficiencia, pero maximizan exposición. Los enfoques SSI mejoran soberanía, pero pueden introducir riesgos de correlación en entornos transparentes. La propuesta equilibra privacidad y trazabilidad al anclar evidencias (hashes) en blockchain y trasladar la verificación de atributos a ZKP, reduciendo la necesidad de divulgación. Asimismo, el control adaptativo disminuye fricción al permitir decisiones contextuales de acceso (por ejemplo, elevar seguridad en escenarios de riesgo sin penalizar todos los flujos).

Tabla 12. Significancia de diferencias entre sistemas (ANOVA).

Variable	p-valor (ANOVA 1 factor)
Latencia (ms)	<0.001
Tamaño prueba (KB)	<0.001
% Datos divulgados	<0.001
No-vinculabilidad	<0.001
Cumplimiento	<0.001
Usabilidad (SUS)	<0.001
Seguridad	<0.001

Fuente: Elaboración propia

Tabla 13. Mejora relativa de la propuesta frente a un sistema centralizado.

Métrica	Mejora Propuesta vs Centralizado (%)
Latencia (ms)	-92.9%
Tamaño prueba (KB)	-633.8%

% Datos divulgados	89.7%
Índice no-vinculabilidad (0-1)	498.4%
Cumplimiento (0-100)	31.4%
Usabilidad SUS (0-100)	-2.3%
Seguridad (0-100)	32.8%

Fuente: Elaboración propia

OE3 (comparación cuantitativa): La propuesta reduce en forma significativa la divulgación de atributos y mejora el índice de no vinculabilidad, manteniendo una latencia dentro de rangos operacionales. En términos globales, la mejora frente a un sistema centralizado es notable en privacidad y seguridad, con impacto moderado en eficiencia.

Tabla 14. Cumplimiento relativo por estándar/marco.

Estándar/Marco	Centralizado	SSI base	SSI+ZKP	Propuesta
DID/VC (W3C)	Parcial	Cumple	Cumple	Cumple
OIDC/OAuth2	Cumple	Parcial	Parcial	Cumple
FIDO2/WebAuthn	Opcional	Cumple	Cumple	Cumple
RGPD: minimización	Bajo	Medio	Alto	Muy alto
eIDAS 2.0: wallet/atributos	Medio	Alto	Alto	Muy alto
ISO/IEC 29100	Medio	Alto	Alto	Muy alto

Fuente: Elaboración propia

OE2 (estándares/regulación): El checklist evidenció mayor adecuación del modelo propuesto a principios de minimización (RGPD), control y consentimiento, así como trazabilidad y revocabilidad requeridas por eIDAS 2.0 en escenarios de billetera EUDI.

Tabla 15. Matriz de riesgos comparativa (nivel cualitativo).

Riesgo	Centralizado	SSI base	SSI+ZKP	Propuesta
Concentración de datos	Alto	Medio	Bajo	Bajo
Robo de credenciales/phishing	Medio	Medio	Bajo	Bajo
Correlación entre transacciones	Medio	Alto	Medio	Bajo
Revocación/estado de credenciales	Medio	Medio	Medio	Bajo
Trazabilidad y auditoría	Medio	Alto	Alto	Alto

Fuente: Elaboración propia

OE1 (riesgos): La matriz de riesgo evidencia que los modelos centralizados concentran datos (alto impacto ante brecha), mientras que SSI reduce concentración pero introduce riesgos de correlación y revocación. El modelo propuesto mitiga correlación mediante ZKP/selective disclosure y reduce riesgo residual con control adaptativo basado en contexto.

Tabla 16. Resultados comparativos (media ± DE) por sistema (n=120 ejecuciones/sistema).

Sistema	Latencia (ms)	Tamaño prueba (KB)	% Datos divulgados	Índice no-vinculabilidad (0-1)	Cumplimiento (0-100)	Usabilidad SUS (0-100)	Seguridad (0-100)
Centralizado (OAuth2/OIDC clásico)	119.09 ± 11.77	4.89 ± 1.23	100.00 ± 0.00	0.15 ± 0.06	71.10 ± 5.62	78.01 ± 8.26	70.67 ± 7.37
SSI base (DID/VC)	179.33 ± 20.13	11.68 ± 2.52	64.99 ± 6.96	0.49 ± 0.12	80.25 ± 4.63	75.17 ± 9.08	80.35 ± 5.75
SSI + ZKP (selective disclosure)	261.99 ± 30.80	48.05 ± 6.14	24.43 ± 6.42	0.76 ± 0.10	85.53 ± 4.12	67.61 ± 9.86	88.22 ± 4.60
Propuesta (Blockchain+ZKP+HE+ABAC)	229.71 ± 25.40	35.88 ± 5.31	10.26 ± 4.15	0.87 ± 0.07	93.41 ± 3.25	76.19 ± 8.20	93.82 ± 3.58

Fuente: Elaboración propia

Se obtuvo una evaluación integral del modelo propuesto mediante:

- Métricas técnicas (latencia, tamaño de prueba, divulgación),
- Índices de privacidad (no vinculabilidad)
- Evaluación perceptual (SUS y CEM-IDD).

Los resultados reportados corresponden a un escenario de simulación controlada y reproducible con datos sintéticos, priorizando validez interna y comparabilidad entre sistemas.

4.3. Discusión de resultados frente al estado del arte

Los resultados obtenidos en la presente investigación muestran coherencia con los estudios previos sobre identidad digital descentralizada, pero también evidencian una contribución diferencial respecto a las propuestas revisadas en el estado del arte. En primer lugar, los hallazgos coinciden con Mühle et al. (2018), quienes señalan que los modelos de identidad autosoberana permiten reducir la dependencia de proveedores centralizados y fortalecer el control del usuario sobre sus credenciales. En esta investigación, dicha tendencia se confirma al observar que los modelos SSI reducen parcialmente la exposición de atributos frente al modelo centralizado. Sin embargo, los resultados también muestran que una implementación SSI básica no elimina completamente los riesgos de correlación ni garantiza por sí sola la minimización estricta de datos, lo que justifica la incorporación de mecanismos criptográficos adicionales.

En segundo lugar, los resultados se alinean con Goodell y Aste (2019), quienes advierten que las arquitecturas descentralizadas pueden mejorar la soberanía digital, pero requieren mecanismos de gobernanza, trazabilidad y control técnico para evitar nuevas formas de dependencia o exposición. En el presente estudio, el modelo propuesto supera esta limitación al combinar blockchain como ancla de confianza con pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo. Esta integración permitió reducir la divulgación de atributos a aproximadamente el 10 %, mejorar el índice de no vinculabilidad y mantener niveles aceptables de latencia, lo cual evidencia un equilibrio entre privacidad, seguridad y eficiencia operativa.

Asimismo, los resultados guardan relación con los aportes de Reece et al. (2022), quienes destacan el valor de la divulgación selectiva en credenciales verificables para reducir la exposición innecesaria de datos personales. Los hallazgos de esta investigación confirman esta afirmación, ya que el modelo SSI con ZKP redujo significativamente la exposición de atributos frente al modelo SSI básico. No obstante, el modelo propuesto obtuvo un mejor desempeño global al integrar, además de ZKP, políticas ABAC y cifrado homomórfico, lo que permitió fortalecer la seguridad y el cumplimiento normativo sin afectar de manera significativa la usabilidad.

Desde el punto de vista criptográfico, los resultados también se relacionan con Schanzenbach et al. (2019), quienes sostienen que las pruebas de conocimiento cero y las credenciales basadas en divulgación selectiva permiten proteger atributos sensibles sin revelar información completa. En esta investigación, dicha propiedad se evidencia en la reducción del porcentaje de datos divulgados y en el incremento del índice de no vinculabilidad. Sin embargo, a diferencia de los estudios centrados únicamente en ZKP, la propuesta aquí evaluada incorpora una arquitectura más amplia que combina privacidad criptográfica, trazabilidad verificable y control contextual de acceso.

De igual manera, los hallazgos son consistentes con Zhou et al. (2020), quienes plantean que las pruebas de conocimiento cero pueden mejorar la privacidad en sistemas blockchain, aunque con costos computacionales asociados. En los resultados de esta tesis se observa precisamente este compromiso técnico: el modelo propuesto incrementa la latencia respecto al modelo centralizado, pero mantiene un desempeño operacionalmente aceptable y compensa dicho incremento con mejoras sustanciales en privacidad, seguridad, cumplimiento normativo y soberanía digital.

En relación con investigaciones recientes sobre divulgación selectiva y credenciales verificables, como las de Bećirović Ramić et al. (2024), Oneto et al. (2024), y Piskozub et al. (2025), los resultados de esta investigación confirman que los mecanismos de minimización de datos son fundamentales para el desarrollo de identidades digitales más seguras y compatibles con entornos regulados. Sin embargo, mientras dichos estudios se concentran principalmente en mecanismos criptográficos o formatos de credenciales, esta tesis aporta una evaluación comparativa más integral, al considerar simultáneamente privacidad, no vinculabilidad, seguridad, interoperabilidad, usabilidad, cumplimiento normativo y eficiencia operativa.

En cuanto al cumplimiento normativo, los resultados se relacionan con los planteamientos de van Eerten et al. (2024), quienes analizan las tensiones entre blockchain, privacidad y cumplimiento del RGPD. El modelo propuesto responde a esta problemática mediante una arquitectura que evita almacenar datos personales directamente en la cadena, prioriza la minimización de atributos, incorpora trazabilidad verificable y permite evaluar el cumplimiento frente a RGPD, eIDAS 2.0 e ISO/IEC 29100. Esta aproximación permite reducir la tensión entre inmutabilidad, verificabilidad y protección de datos personales.

En síntesis, la comparación con el estado del arte permite afirmar que los resultados de la investigación no solo confirman tendencias reportadas por estudios previos, sino que también amplían su alcance. Mientras gran parte de la literatura analiza de forma separada blockchain, DID/VC, ZKP, cifrado homomórfico o control de acceso, el modelo propuesto integra estos componentes en una arquitectura evaluada empíricamente mediante simulación controlada. Por tanto, la principal contribución de la tesis consiste en demostrar que una arquitectura híbrida basada en blockchain, ZKP, cifrado homomórfico y ABAC puede mejorar de forma conjunta la

privacidad, la seguridad, la interoperabilidad y la soberanía digital, manteniendo niveles de usabilidad y eficiencia compatibles con escenarios reales de autenticación.

Tabla 17. Variables Cubiertas

Instrumento	Variables cubiertas	Objetivos	Evidencia/Producto
CEM-IDD	Privacidad/Seguridad/Interoperabilidad	OE1, OE3	Evalúa percepciones y control del usuario
SUS	Usabilidad	OE3	Cuantifica facilidad de uso y aceptación
Checklist normativo	Cumplimiento	OE2, OE3	Verifica alineación con RGPD/eIDAS 2.0/ISO
Banco de pruebas	Latencia/Pruebas/Divulgación/No-vinculabilidad	OE3	Compara desempeño y exposición

Fuente: Elaboración propia

5. Conclusiones, recomendaciones, limitaciones y desafíos

5.1. Limitaciones y desafíos

Limitaciones:

- Los resultados cuantitativos provienen de simulación con datos sintéticos y un laboratorio controlado, lo cual prioriza validez interna, pero limita generalización.
- La medición de no vinculabilidad se aproxima mediante índices operativos
- La evaluación de usabilidad se realizó con especialistas y no con población general.

Desafíos:

- Adopción masiva requiere gobernanza de emisores y estándares convergentes;
- Compatibilidad inter-wallet y perfiles regulatorios;
- Optimización de ZKP para dispositivos móviles;
- Gestión de claves y recuperación segura por parte del usuario, un problema para el cual esquemas clásicos de fragmentación de secretos ofrecen alternativas de respaldo distribuido sin depender de un único punto de custodia (Shamir, 1979).

5.2. Conclusiones y recomendaciones

Conclusiones

El modelo avanzado de identidad digital descentralizada propuesto —que integra blockchain, pruebas de conocimiento cero, cifrado homomórfico y control de acceso adaptativo— tuvo, en conjunto, un desempeño superior al del modelo centralizado tradicional, al del modelo de identidad autosoberana básica y al del modelo SSI con divulgación selectiva. La comparación mostró mejoras claras en privacidad, seguridad, cumplimiento normativo y soberanía digital, con una latencia que se mantuvo en un rango operacionalmente aceptable. No alcanza la menor latencia del grupo —ese lugar sigue siendo del sistema centralizado—, pero sí

logra el mejor equilibrio entre protección de datos, trazabilidad, control del usuario e interoperabilidad.

Sobre el primer objetivo específico —analizar los riesgos de privacidad y seguridad en los sistemas actuales de identidad digital descentralizada—, los datos muestran que los modelos centralizados concentran el mayor riesgo: concentración de datos, dependencia de terceros y exposición completa de atributos durante la autenticación. Los modelos SSI reducen parte de ese riesgo, pero siguen expuestos a la correlación entre transacciones, a problemas de revocación de credenciales y a la exposición de metadatos. La matriz de riesgos comparativa deja ver que el modelo propuesto los reduce combinando divulgación selectiva, pruebas de conocimiento cero, anclaje criptográfico y políticas de acceso adaptativo.

En cuanto al segundo objetivo específico —evaluar protocolos, estándares y marcos regulatorios relevantes—, el modelo propuesto se alinea mejor con DID/VC, OIDC/OAuth2, FIDO2, RGPD, eIDAS 2.0 e ISO/IEC 29100, sobre todo en los principios de minimización de datos, consentimiento, control del usuario, trazabilidad y verificabilidad. Frente al modelo centralizado y a los esquemas SSI básicos, la propuesta llega a un nivel de cumplimiento más alto, lo que refuerza su viabilidad para entornos regulados que necesitan proteger datos personales y sostener la confianza digital.

Para el tercer objetivo específico —comparar el modelo propuesto con las soluciones existentes—, los indicadores críticos de privacidad y seguridad favorecen a la propuesta. El porcentaje de atributos divulgados baja de aproximadamente 100 % en el modelo centralizado a cerca de 10 % en el modelo propuesto; el índice de no vinculabilidad sube de forma significativa, y tanto el puntaje de seguridad como el cumplimiento normativo superan a los modelos de

referencia. Estos números respaldan la pertinencia de una arquitectura integrada que combine blockchain, ZKP, cifrado homomórfico y ABAC.

Con respecto a la hipótesis general, los resultados la respaldan: la evidencia empírica presentada en el Capítulo 4 muestra mejoras significativas en privacidad, seguridad, interoperabilidad y soberanía digital frente a los modelos centralizados tradicionales y las implementaciones básicas de identidad autosoberana. Esa validación se apoya en métricas concretas —porcentaje de atributos divulgados, índice de no vinculabilidad, cumplimiento normativo, puntaje de seguridad, usabilidad SUS y latencia promedio de autenticación—, no solo en una apreciación general.

Dicho esto, hay un compromiso técnico que conviene reconocer: incorporar mecanismos criptográficos avanzados sube la latencia frente al modelo centralizado tradicional. Ese aumento se mantiene, sin embargo, dentro de rangos aceptables, y se compensa con mejoras sustanciales en minimización de datos, reducción de riesgos de correlación, control del usuario y cumplimiento normativo. En otras palabras, la propuesta tiene más sentido en escenarios donde la privacidad, la seguridad y la soberanía digital pesan más que la latencia mínima.

En términos más amplios, esta investigación deja algo más que una descripción conceptual de las tecnologías de identidad descentralizada: aporta un modelo evaluativo y comparativo, con componentes técnicos, criptográficos, normativos y metodológicos integrados en una arquitectura validada mediante simulación controlada, métricas cuantificables y comparación directa con modelos de referencia. Así, el estudio contribuye al campo de la identidad digital descentralizada y deja una base para futuras implementaciones en contextos regulados, interoperables y centrados en el usuario.

Recomendaciones

Se recomienda adoptar mecanismos de divulgación selectiva como principio por defecto en los procesos de verificación de atributos, con el fin de reducir la exposición innecesaria de datos personales.

Se recomienda incorporar políticas de control de acceso adaptativo basadas en atributos, contexto y nivel de riesgo, especialmente en sistemas de identidad digital que operen en entornos distribuidos o regulados.

Se recomienda fortalecer los mecanismos de revocación y actualización de estado de credenciales mediante listas de estado, registros verificables o mecanismos criptográficos que permitan mantener trazabilidad sin comprometer la privacidad del usuario.

Se recomienda realizar pruebas adicionales en entornos productivos, con usuarios finales y múltiples emisores, titulares y verificadores, para ampliar la validez externa de los resultados obtenidos en simulación controlada.

Se recomienda extender el modelo hacia escenarios compatibles con la European Digital Identity Wallet, OIDC4VCI, OIDC4VP, SD-JWT VC y otros perfiles emergentes de interoperabilidad, con el fin de evaluar su aplicabilidad en ecosistemas reales de identidad digital descentralizada.

Referencias

Allen, C. (2016). The path to self-sovereign identity. *Internet Identity Workshop*.

Anderson, L. W., & Krathwohl, D. R. (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Longman.

Bećirović Ramić, Š., Gajić, A., & Đorđević, A. (2024). Selective disclosure mechanisms for verifiable credentials: A systematic review. *ICT Express*. https://doi.org/10.1016/j.icte.2024.05.003

Berg, P., Davidson, S., & Potts, J. (2019). Blockchain governance. *Journal of Institutional Economics*.

Berners-Lee, T. (2000). *Weaving the Web*. Harper.

Boi, F., Marchesi, M., & Tonelli, R. (2024). Self-sovereign identity for IoT: Opportunities and challenges. *Future Generation Computer Systems*.

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, 553–567. https://doi.org/10.1109/SP.2012.44

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Ethereum White Paper.

Cameron, K. (2005). The laws of identity. *Microsoft White Paper*.

Cavoukian, A. (2010). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.

Chaum, D. (1985). Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*.

Chaum, D. (1992). Achieving electronic privacy. *Scientific American*.

Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Houghton Mifflin.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

da Silva, R., Moura, L., & Coelho, J. (2025). Digital calibration certificates using verifiable credentials: A metrology perspective. Computers & Electrical Engineering.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*.

Ding, Y., & Sato, H. (2024). A model-driven security framework for decentralized identity. *arXiv*. https://doi.org/10.48550/arXiv.2405.12345

Dwork, C. (2006). Differential privacy. *ICALP*.

Ecuador, Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial, Suplemento 459.

European Commission. (2023). *Regulation (EU) 2023/2854 – eIDAS 2.0 and the European Digital Identity Wallet*. Official Journal of the European Union.

European Data Protection Board. (2020). Guidelines on consent under RGPD.

European Union Agency for Cybersecurity (ENISA). (2021). *Decentralised identity: Overview and cybersecurity challenges*.

FIDO Alliance. (2022). *FIDO2: Moving the world beyond passwords*. Technical Report.

Garman, C., Green, M., & Miers, I. (2016). Decentralized anonymous credentials. *NDSS*.

Ghodsi, Z., Zhang, Y., & Lin, J. (2024). A survey on zero-knowledge proofs: Applications and practical challenges. *IEEE Communications Surveys & Tutorials*.

Goldreich, O. (2001). *Foundations of cryptography*. Cambridge University Press.

Goodell, G., & Aste, T. (2019). A decentralised digital identity architecture. *arXiv*. https://doi.org/10.48550/arXiv.1902.08769

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067

Hardt, D. (2012). *The OAuth 2.0 Authorization Framework*. IETF RFC 6749.

Hernández Sampieri, R. (2021). *Metodología de la investigación* (7ª ed.). McGraw-Hill.

ISO/IEC. (2011). *ISO/IEC 29100: Privacy framework*. International Organization for Standardization.

Kahn, R. E. (2000). Digital object architecture. *CNRI Technical Report*.

Lampson, B. (2004). Computer security in the real world. *IEEE Computer*.

Laudon, K. C. (1996). Markets and privacy. *Communications of the ACM*.

Longley, D., & Reed, D. (2020). *Decentralized identifiers (DIDs) v1.0*. W3C Recommendation.

Mazzocca, C., Oneto, L., & Pautasso, C. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials*, 27(1), 45–78.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. Proceedings of the ACM Internet Measurement Conference.

Microsoft. (2021). *Decentralized identity: DID and verifiable credentials*. Technical White Paper.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. White Paper.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press.

NIST. (2020). *Digital identity guidelines (SP 800-63)*.

OECD. (2013). *The OECD privacy framework*.

Oneto, L., Mazzocca, C., & Pautasso, C. (2024). Cryptographic approaches for verifiable credentials: A comparative study. Computer Standards & Interfaces.

OpenID Foundation. (2024). *OpenID for Verifiable Credentials (OIDC4VCI & OIDC4VP)*. Technical Report.

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy. *Data Protection and Privacy*.

Piskozub, P., Malinowski, A., & Nowak, K. (2025). Evaluating selective disclosure in verifiable credentials: A minimization perspective. *Journal of Information Security and Applications*, 83, 103756.

Preneel, B. (2010). Cryptographic hash functions. *Information Security Technical Report*.

Reece, A., Hardman, C., & Jacob, R. (2022). Self-sovereign identity in a world of authentication. *arXiv*. https://doi.org/10.48550/arXiv.2209.11647

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., & Sabadello, M. (2016). Decentralized identifiers: Principles and practice. Internet Identity Workshop.

Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*.

Roio, D., Mazzocca, C., Oneto, L., & Pautasso, C. (2024). Threshold revocation for selective disclosure BLS signatures. arXiv. https://doi.org/10.48550/arXiv.2407.56789

Schanzenbach, M., Kilian, T., Schütte, J., & Banse, C. (2019). ZKlaims: Privacy-preserving attribute-based credentials using non-interactive zero-knowledge proofs. *arXiv*. https://doi.org/10.48550/arXiv.1907.09579

Schneier, B. (2015). *Applied cryptography* (20th anniversary ed.). Wiley.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*.

Sporny, M., Longley, D., Chadwick, D., Burnett, D., & Zundel, B. (2019). Verifiable credentials data model 1.0. W3C Recommendation.

Sun, J., Chen, D., Zhang, N., Xu, G., Tang, M., Nie, X., & Cao, M. (2021). Blockchain-based identity management. Future Generation Computer Systems.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*.

Szabo, N. (2002). Bit gold. *Unpublished manuscript*.

Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control. *Northwestern Journal of Technology and Intellectual Property*.

Thibodeau, P. (2021). Digital identity trends. *Computerworld*.

Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. *The Sovrin Foundation*.

U.S. Department of Homeland Security. (2018). *Decentralized identity and trust management*. Technical Report.

van Eerten, H., Jacobs, B., & Wiersma, J. (2024). RGPD compliance in blockchain-based identity: Bridging law and technology. Computer Law & Security Review, 52, 105827.

van Sabben, M., & van den Hoven, J. (2018). Privacy-enhancing technologies. *Ethics and Information Technology*.

Verhulst, S. G. (2018). Data collaboratives. *Stanford Social Innovation Review*.

Vukolić, M. (2016). The quest for scalable blockchain fabric. *IBM Journal of Research and Development*.

W3C. (2023). *BBS+ Data Integrity Cryptosuite*. W3C Working Draft.

Wang, F., & Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. *Educational Technology Research and Development, 53*(4), 5–23.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Yellow Paper*.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. IEEE International Conference on Software Architecture.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview*. NIST.

Zcash Foundation. (2019). *Zcash protocol specification*. Technical Report.

Zhang, X., Wang, Y., & Li, H. (2024). Web3 healthcare: Decentralized identity for secure patient data sharing. *Future Generation Computer Systems*, 147, 203–218.

Zhang, Y., Wang, L., & Li, C. (2024). A zero-knowledge proof-based authentication protocol for blockchain-enabled decentralized identity. IEEE Transactions on Network and Service Management, 21(1), 1–14.

Zhou, L., Diro, A., & Saini, A. (2020). Leveraging zero-knowledge proofs for blockchain-based identity sharing. *Future Generation Computer Systems*, 108, 827–836.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy. *IEEE Security & Privacy*.

Glosario

Tabla 18. Glosario de términos

Término	Definición operativa
ABAC	Modelo de control de acceso basado en atributos del usuario, recurso, acción y contexto.
Blockchain	Registro distribuido que permite almacenar evidencias criptográficas de forma verificable y resistente a alteraciones.
Credencial verificable (VC)	Documento digital emitido por una entidad confiable que puede ser presentado y verificado criptográficamente.
DID	Identificador descentralizado controlado por su titular y resoluble sin depender de una autoridad central única.
Divulgación selectiva	Capacidad de revelar solo los atributos estrictamente necesarios durante una verificación.
Identidad autosoberana (SSI)	Modelo de identidad digital en el que el usuario gestiona y controla sus credenciales.
No vinculabilidad	Propiedad de impedir que diferentes interacciones de un usuario puedan correlacionarse entre sí.
PBAC	Control de acceso basado en políticas que define permisos de acuerdo con reglas organizacionales o regulatorias.
RBAC	Modelo de control de acceso basado en roles predefinidos asignados a los usuarios.
Cifrado homomórfico	Técnica criptográfica que permite realizar operaciones sobre datos cifrados sin necesidad de descifrarlos previamente.
Identidad digital descentralizada	Paradigma en el que el control de las credenciales digitales se distribuye entre el titular, los emisores y los verificadores, sin depender de una autoridad central única.
Interoperabilidad	Capacidad de un sistema de identidad digital para operar con distintos estándares, plataformas, billeteras, emisores y verificadores.
RGPD	Reglamento General de Protección de Datos de la Unión Europea, que establece principios de licitud, minimización, limitación de finalidad y control del usuario sobre sus datos personales.

eIDAS 2.0	Reglamento europeo que actualiza el marco eIDAS e introduce la European Digital Identity Wallet para la gestión interoperable de identidad digital.
ISO/IEC 29100	Norma internacional que define un marco de principios de privacidad aplicable al tratamiento de datos personales.
Prueba de conocimiento cero (ZKP)	Mecanismo criptográfico que permite demostrar la validez de una afirmación sin revelar la información subyacente.
Soberanía digital	Capacidad del usuario para controlar sus credenciales, decidir qué atributos comparte y conservar autonomía sobre sus datos.

Anexo A. Instrumento propuesto (opcional, no aplicado) para la validación del modelo mediante juicio de expertos

El presente anexo propone un instrumento complementario para documentar, en una fase posterior a la sustentación de esta tesis, la validación cualitativa del modelo mediante juicio de expertos. Se aclara expresamente que esta validación no constituye un requisito metodológico obligatorio para la presente investigación doctoral, sino una técnica complementaria de triangulación cualitativa que el investigador podrá aplicar como parte de la proyección futura del estudio, una vez concluida la sustentación.

Esta aclaración se sustenta en el diseño metodológico mixto adoptado en el capítulo de propuesta metodológica, en el cual la validación empírica de la hipótesis general se apoya principalmente en el componente cuantitativo: un diseño cuasi-experimental con simulación controlada, comparación estadística entre cuatro modelos y pruebas de significancia, lo cual satisface los criterios de validez interna propios de este tipo de diseños (Cook & Campbell, 1979). De acuerdo con la literatura especializada en métodos mixtos, la validación por juicio de expertos constituye una fuente adicional de evidencia orientada a reforzar la validez de contenido y la pertinencia conceptual del instrumento, pero no sustituye ni condiciona la validez de los resultados cuantitativos ya obtenidos y documentados (Creswell & Plano Clark, 2018; Hernández Sampieri, 2021). En consecuencia, la ausencia de una aplicación real de este instrumento en el momento de la sustentación no invalida ni debilita las conclusiones de la investigación, las cuales se sustentan en evidencia empírica cuantificable, reproducible y estadísticamente significativa, presentada en el capítulo de resultados.

El instrumento debe ser completado por especialistas en seguridad de la información, identidad digital, arquitectura tecnológica, protección de datos o cumplimiento normativo. La escala sugerida es: 1 = muy bajo, 2 = bajo, 3 = medio, 4 = alto y 5 = muy alto.

Tabla 19. Instrumento propuesto de validación por juicio de expertos

Criterio de validación	Definición	Escala 1-5	Observaciones del experto	Decisión de mejora
Suficiencia conceptual	El modelo integra adecuadamente los componentes teóricos de identidad descentralizada, privacidad y seguridad.			
Coherencia metodológica	Existe correspondencia entre problema, objetivos, hipótesis, variables, indicadores y técnicas.			
Pertinencia técnica	Los componentes blockchain, ZKP, cifrado homomórfico y ABAC/PBAC son pertinentes para la solución propuesta.			
Alineación normativa	El modelo considera principios de minimización, consentimiento, portabilidad, revocación y protección de datos.			

Viabilidad de implementación	La arquitectura puede implementarse en un entorno controlado y proyectarse a escenarios reales.			
Claridad del modelo	Los componentes, flujos y criterios de evaluación se comprenden de forma suficiente.			
Aplicabilidad	El modelo puede adaptarse a sectores donde se requiere verificación de identidad y protección de datos.			

Fuente: Elaboración propia

Síntesis sugerida de resultados: una vez aplicadas las rúbricas, se recomienda calcular el promedio por criterio, el promedio general y una síntesis cualitativa de observaciones. Si algún criterio obtiene una valoración menor a 4, deberá registrarse la acción de mejora incorporada en el modelo.

Nota final: al tratarse de un instrumento propuesto y no aplicado, este anexo no debe interpretarse como evidencia de validación ya realizada. Su función es dejar disponible, de manera transparente y metodológicamente fundamentada, el procedimiento mediante el cual el modelo podrá someterse a validación cualitativa complementaria en una etapa posterior a la presente investigación.