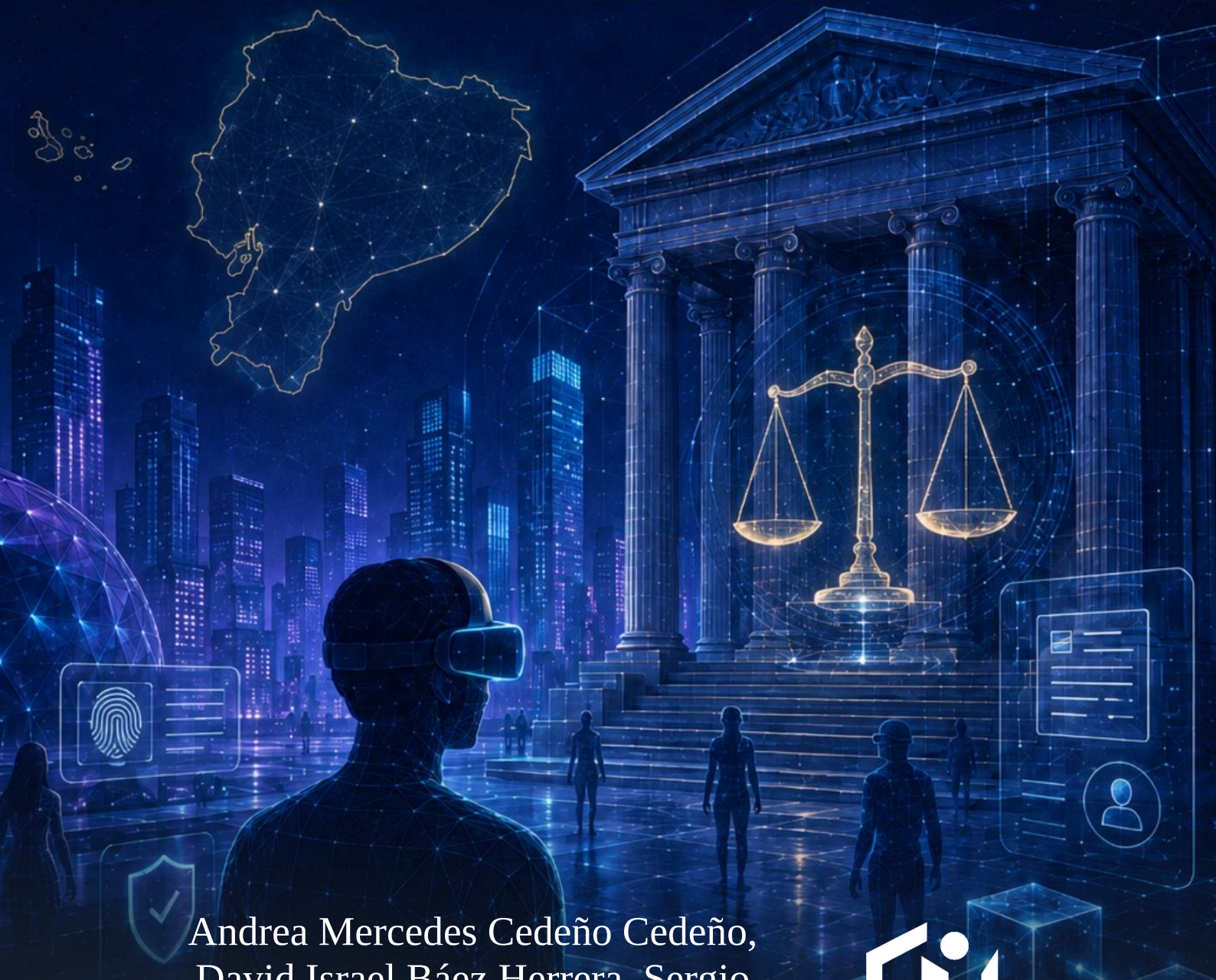
Derecho y metaverso

frente a los desafíos de los mundos virtuales



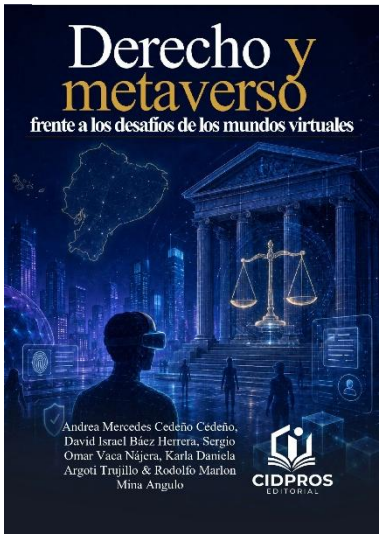
Andrea Mercedes Cedeño Cedeño, David Israel Báez Herrera, Sergio Omar Vaca Nájera, Karla Daniela Argoti Trujillo & Rodolfo Marlon Mina Angulo

CIDPROS
EDITORIAL

Derecho y metaverso frente a los desafíos de los mundos virtuales

Andrea Mercedes Cedeño Cedeño, David Israel Báez Herrera, Sergio Omar Vaca Nájera, Karla Daniela Argoti Trujillo & Rodolfo Marlon Mina Angulo





Datos bibliográficos

ISBN	978-9907-848-12-0
Título del libro	Derecho y metaverso frente a los desafíos de los mundos virtuales
Autores	Andrea Mercedes Cedeño Cedeño David Israel Báez Herrera Sergio Omar Vaca Nájera Karla Daniela Argoti Trujillo Rodolfo Marlon Mina Angulo
Editorial	CIDPROS EDITORIAL
Materia	340 - Derecho
Público objetivo	Profesional / académico
Año	2026
Número de edición	1
Tamaño	3.12Mb
Soporte	Libro digital descargable
Formato	PDF (.pdf)
Idioma	Español
DOI	https://doi.org/10.70577/v62jrk27

Hecho en Ecuador / Made in Ecuador

MSc. Andrea Mercedes Cedeño Cedeño

Investigadora Independiente
ab.andreacedeno@hotmail.com
https://orcid.org/0009-0009-6139-6532
Portoviejo, Manabí, Ecuador

Semblanza



Andrea M. Cedeño Cedeño, abogada ecuatoriana nacida el 08 de abril de 1986 en el cantón Portoviejo, desde su infancia, ha mantenido su residencia en el sector de Pachinche Afuera, comunidad de tradición eminentemente agrícola; crecer en este entorno rural contribuyó, desde temprana edad, a fortalecer su sensibilidad social y a forjar una visión humanista del Derecho, concebido como una herramienta al servicio de la justicia y del bien común. Su cercanía con las dinámicas, necesidades y realidades de la comunidad le permitió desarrollar una profunda empatía social, consolidando un firme compromiso con la justicia, la equidad y la promoción del desarrollo social.

Cuenta con una sólida formación académica. Es Tecnóloga Programadora y Abogada; posteriormente obtuvo, en el extranjero, el título de Máster en Derecho del Trabajo y de la Seguridad Social. Actualmente, cursa una Maestría en Derecho Procesal Constitucional. Esta trayectoria académica evidencia su vocación por la excelencia profesional, así como su compromiso con la actualización constante y el fortalecimiento de sus conocimientos en el ámbito de las ciencias jurídicas.

A lo largo de su trayectoria personal y profesional, se ha distinguido por su compromiso con el servicio a la sociedad. En el ámbito del voluntariado, ha colaborado con la ONG Plan International, organización dedicada a la promoción y protección de los derechos de la niñez y a la construcción de sociedades más igualitarias para niñas, niños y adolescentes.

En el sector público, desarrolla su trayectoria en el ámbito de la Función Judicial desde el año 2012, desempeñándose como funcionaria judicial en la Corte Provincial de Justicia de Manabí, donde ha ejercido sus responsabilidades con compromiso, profesionalismo y sentido de servicio.

MSc. David Israel Báez Herrera

Investigador Independiente
dbmasternet@gmail.com
https://orcid.org/0009-0009-2487-7214
Quito, Pichincha, Ecuador

Semblanza



David Israel Báez Herrera es un investigador y profesional ecuatoriano residente en Quito, especializado en tecnologías de la información, transformación digital, gestión de proyectos e innovación educativa. Cuenta con un Bachelor of Arts (BA) en Redes y Sistemas Operativos, una maestría en Telecomunicaciones y una maestría en Innovación Educativa.

Actualmente cursa un Doctorado en Dirección de Proyectos, en el que desarrolla una investigación orientada al fortalecimiento de los procesos de evaluación interna y acreditación de las instituciones de educación superior mediante un modelo apoyado en una plataforma digital para la gestión, validación y análisis de evidencias. Posee más de diez certificaciones internacionales y acreditaciones de formación especializada en tecnologías, metodologías y estándares promovidos por organizaciones reconocidas como Cisco, Amazon Web Services (AWS), Red Hat, WatchGuard, Microsoft y Hewlett Packard (HP), además de formación en gestión de proyectos bajo el enfoque PMP y en sistemas de gestión basados en normas ISO.

Su preparación comprende áreas como redes, ciberseguridad, telecomunicaciones, computación en la nube, desarrollo de software, bases de datos, infraestructura tecnológica, sistemas operativos y dirección de proyectos. También cuenta con formación y certificaciones relacionadas con los sistemas de gestión de la calidad ISO 9001 y de seguridad de la información ISO/IEC 27001, así como una certificación como Delegado de Protección de Datos, conocimientos que le han permitido intervenir en iniciativas de calidad, seguridad digital, privacidad, protección de datos personales y cumplimiento normativo. Su perfil académico se complementa con más de 150 cursos de formación continua, cuatro diplomados vinculados con programación, investigación científica e inteligencia artificial y la participación en seminarios internacionales relacionados con sus áreas de especialización.

A lo largo de más de quince años de trayectoria, ha asesorado y acompañado a organizaciones públicas y privadas de los sectores educativo, financiero, bancario, inmobiliario, de la construcción y del desarrollo tecnológico en proyectos de infraestructura, redes, telecomunicaciones, seguridad informática y transformación

digital. En el ámbito de la educación superior, ha liderado y participado en la implementación de soluciones de software a medida para la gestión académica, administrativa y contable, contribuyendo a la automatización de actividades, la integración de información, la generación de indicadores y el fortalecimiento de la toma de decisiones institucionales. Su experiencia también comprende el diseño instruccional de contenidos y entornos virtuales de aprendizaje, la administración de plataformas educativas, el desarrollo de sistemas de información, la mejora y optimización de procesos y la implementación, mantenimiento y evaluación de sistemas de gestión de la calidad. Su ejercicio profesional se caracteriza por integrar la tecnología, la educación, la investigación y la gestión organizacional desde una perspectiva interdisciplinaria orientada a la innovación, la mejora continua, la seguridad de la información y el cumplimiento normativo.

Mantiene un firme compromiso con la ética profesional, la actualización permanente y la generación de soluciones tecnológicas que contribuyan a elevar la calidad educativa, fortalecer la eficiencia de las organizaciones y producir un impacto positivo y sostenible en la sociedad.

Mgs. Sergio Omar Vaca Nájera

Investigador Independiente
svn.98sv@gmail.com
https://orcid.org/0009-0005-7570-5309
Quito, Pichincha, Ecuador

Semblanza



Sergio Omar Vaca Nájera es abogado, investigador y docente ecuatoriano, nacido el 12 de agosto de 1998 en la ciudad de Quito. Su trayectoria se ha construido a partir de una profunda vocación por el Derecho, la defensa de los derechos humanos, la justicia constitucional y el servicio público. A lo largo de su formación y experiencia profesional ha procurado integrar el ejercicio jurídico con la investigación y la docencia, convencido de que el conocimiento adquiere verdadero sentido cuando contribuye a comprender y transformar las realidades sociales.

Es Abogado de los Tribunales y Juzgados de la República del Ecuador y cuenta con tres programas de maestría culminados: Magíster en Derechos Humanos con mención en Sistemas Internacionales de Protección, Magíster en Derecho con mención en Derecho Procesal Penal y Magíster en Derecho con mención en Derecho Constitucional. Actualmente continúa fortaleciendo su formación interdisciplinaria mediante una cuarta maestría en Criminalística y Ciencias Forenses en la Universidad Estatal de Milagro y, paralelamente, desarrolla estudios de Doctorado (PhD) en Derecho en la Universidad Nacional de Mar del Plata, Argentina. Esta preparación ha fortalecido significativamente sus capacidades de análisis crítico, investigación, gestión, liderazgo y planificación estratégica.

En el ámbito profesional, ha desempeñado cargos dentro de la Fiscalía General del Estado y la Defensoría Pública, destacando por su proactividad, responsabilidad y entrega en la búsqueda de la justicia. Su experiencia se complementa con la docencia en educación superior, espacio desde el cual ha contribuido a la formación de estudiantes en áreas relacionadas con la ética, la legislación y la realidad contemporánea.

Su vocación investigativa se refleja en su participación como coautor de diversas publicaciones científicas, entre ellas: “Conciencia metacognitiva de estrategias de lecturas y comprensión percibida en bachillerato”; “La protección de datos personales como derecho constitucional autónomo en la jurisprudencia ecuatoriana”; “Ejecución

de sentencias de la Corte Constitucional en derechos humanos: revisión bibliográfica"; y "Jurisprudencia sobre inteligencia artificial y responsabilidad jurídica". Estas investigaciones evidencian un interés académico amplio e interdisciplinario, orientado al estudio de los derechos humanos, el constitucionalismo, la efectividad de las decisiones jurisdiccionales y los nuevos desafíos que plantea la tecnología para el Derecho.

Su trayectoria representa una búsqueda constante de crecimiento intelectual y profesional. Para Sergio Omar Vaca Nájera, la formación académica no constituye únicamente la acumulación de títulos, sino un compromiso permanente con el aprendizaje, la reflexión crítica y la generación de conocimiento. Por ello, concibe la escritura y la investigación como espacios de diálogo capaces de trascender el ámbito individual y contribuir a la construcción de un Derecho más humano, responsable y comprometido con los desafíos de la sociedad contemporánea.

Ab. Karla Daniela Argoti Trujillo

Abogada de los tribunales y juzgados de la república del ecuador
argotikarla@gmail.com
https://orcid.org/0009-0001-1026-3272
Quito, Pichincha, Ecuador

Semblanza



Karla Daniela Argoti Trujillo es abogada ecuatoriana con cinco años de experiencia en asesoría legal integral y gestión de procesos judiciales y administrativos, con orientación al sector corporativo. Su trayectoria profesional integra el derecho societario, la protección de datos personales, el derecho administrativo y laboral, así como la cobranza judicial y recuperación de cartera.

Es Abogada de los Tribunales y Juzgados de la República del Ecuador por la Universidad Central del Ecuador. Actualmente cursa la Maestría en Derecho Administrativo en la Universidad ECOTEC.

Se ha desempeñado como Procuradora Judicial en varias empresas comerciales donde ha liderado la implementación de esquemas documentales para operaciones de venta a crédito, estrategias de defensa en procesos administrativos sancionadores, la función interna de protección de datos personales y la elaboración de instrumentos jurídicos corporativos de alta relevancia. Ha representado a organizaciones ante el Ministerio de Producción, Comercio Exterior, Inversiones y Pesca, la Defensoría del Pueblo y el Ministerio de Trabajo.

Previamente ejerció como abogada en el Consultorio Jurídico Legis Actio, brindando asesoría legal integral en derecho civil y de familia, y trabajó en la protección de grupos prioritarios —adultos mayores— en los Centros de Atención al Adulto Mayor del IESS, donde patrocinó acciones de protección constitucional.

Su formación complementaria incluye cursos especializados en constitución de compañías y estructuras patrimoniales, derecho laboral especializado, derecho societario y ley de protección de datos personales. Se distingue por sus fortalezas en negociación, resolución de conflictos, argumentación jurídica, redacción de instrumentos legales y atención al detalle.

MSc. Rodolfo Marlon Mina Angulo

Universidada Tecnica Luis Vargas Torres
marlon.mina.angulo@utelvt.edu.ec
https://orcid.org/0000-0002-5823-1034
Esmeraldas, Esmeraldas, Ecuador.

Semblanza



Rodolfo Marlon Mina Angulo es un docente nacido el 25 de sagosto de 1976 en Esmeraldas, cuya vida ha estado marcada por su residencia en el cantón Esmerladas, un entorno urbano que fortaleció su amor por la educacion y su visión humanista de la docencia como instrumento al servicio del bien común. Desde temprana edad desarrolló una profunda empatía por la situación de la juventud y adolecia lo que ha orientado su compromiso con este sector de la sociedad esmerladeña y ecuatoriana, la equidad y el desarrollo social.

Cuenta con una sólida formación académica: es Tecnologo Programador de Sistemas, Licenciado en Informatica Educativa y catedratico de la Universidad Tecnica Luis Vargas Torres de Esmeraldas desde 2018. Posteriormente obtuvo el título de Magíster en Ingenieria de Software y Sistemas Informaticos en España. Esta preparación refleja su vocación por la excelencia académica y la actualización permanente en las ciencias pedagogica.

A lo largo de su trayectoria, ha destacado tanto en su vida personal como en el servicio público, promoviendo principios,valores, equidad y con enfoque de vida, basada en la dignidad humana y el respeto a los derechos fundamentales de una sociedaad mas justa y equitativa. Su vocación académica se evidencia en artículos como “Estrategias Innovadoras Para Mitigar la Suplantación de Identidad en Redes Sociales” y el libro “Principios Fundamentales para la Iniciación de la Investigación Científica.”. Padre y profesional comprometido, representa valores de resiliencia, ética e integridad, inspirando a nuevas generaciones a construir un Ecuador más justo y solidario donde la juventud sean mas criticos, autocriticos, refexiva y analitica.

El contenido y las ideas expuestas en esta obra se encuentran protegidos por la normativa vigente en materia de propiedad intelectual y constituyen derechos exclusivos de su(s) autor(es).

Derechos de Autor © 2026

Este documento se publica bajo los términos y condiciones de la licencia:



Creative Commons Reconocimiento – No Comercial – Compartir Igual 4.0 Internacional (CC BY-NC-SA 4.0)

Usted es libre de compartir y adaptar el material, siempre que otorgue el crédito correspondiente, no lo utilice con fines comerciales y distribuya sus contribuciones bajo la misma licencia.

Para ver una copia de esta licencia, visite: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es

Sinopsis

El metaverso representa una nueva etapa en la evolución de los entornos digitales, al integrar realidad virtual y aumentada, avatares, inteligencia artificial, sensores, cadenas de bloques, activos digitales y sistemas automatizados. Estas tecnologías permiten desarrollar actividades sociales, educativas, laborales, comerciales y recreativas dentro de espacios persistentes capaces de producir consecuencias jurídicas más allá de la experiencia virtual.

Esta obra analiza los principales desafíos que el metaverso plantea al derecho, con especial atención al ordenamiento jurídico ecuatoriano. Se examinan la identidad digital, los avatares, la protección de datos personales y biométricos, el consentimiento, la intimidad, la libertad de expresión, la protección de menores, la suplantación de identidad y el hábeas data. Asimismo, se estudian la economía virtual, los bienes digitales, la propiedad de activos, los NFT, los contratos electrónicos e inteligentes, la protección del consumidor, la propiedad intelectual y la tributación de operaciones virtuales.

El libro también aborda la responsabilidad jurídica por daños, la actuación de las plataformas, los delitos cometidos en mundos virtuales, el acoso mediante avatares, el fraude, la ciberseguridad y la evidencia digital. Desde una perspectiva de gobernanza, se analizan la jurisdicción, la cooperación internacional, los derechos humanos, la transparencia algorítmica, la inclusión y la sostenibilidad.

La obra sostiene que el metaverso no constituye un espacio independiente del derecho. Aunque las normas vigentes ofrecen bases para resolver numerosos conflictos, sus características inmersivas, automatizadas y transfronterizas exigen criterios específicos de interpretación, prevención y responsabilidad. Finalmente, se propone una regulación futura para Ecuador basada en riesgos, protección efectiva de derechos, transparencia tecnológica y cooperación institucional.

Palabras clave: metaverso; derecho digital; identidad digital; responsabilidad jurídica; regulación ecuatoriana.

Synopsis

The metaverse represents a new stage in the evolution of digital environments by integrating virtual and augmented reality, avatars, artificial intelligence, sensors, blockchain technologies, digital assets, and automated systems. These technologies enable social, educational, professional, commercial, and recreational activities to take place within persistent spaces capable of producing legal consequences beyond the virtual experience.

This book examines the main challenges that the metaverse poses to the law, with particular attention to the Ecuadorian legal system. It addresses digital identity, avatars, the protection of personal and biometric data, consent, privacy, freedom of expression, the protection of minors, identity impersonation, and habeas data. It also explores the virtual economy, digital goods, ownership of assets, NFTs, electronic and smart contracts, consumer protection, intellectual property, and the taxation of virtual transactions.

The book also discusses legal liability for damages, the role of platforms, crimes committed in virtual worlds, harassment through avatars, fraud, cybersecurity, and digital evidence. From a governance perspective, it analyzes jurisdiction, international cooperation, human rights, algorithmic transparency, inclusion, and sustainability.

The book argues that the metaverse does not constitute a space independent from the law. Although existing rules provide a basis for resolving numerous disputes, its immersive, automated, and cross-border characteristics require specific standards of interpretation, prevention, and liability. Finally, it proposes a future regulatory framework for Ecuador based on risk, effective protection of rights, technological transparency, and institutional cooperation.

Keywords: metaverse; digital law; digital identity; legal liability; Ecuadorian regulation.

ÍNDICE

Sinopsis 12

Synopsis 13

Introducción 16

Capítulo 1 Fundamentos jurídicos y tecnológicos del metaverso 20

1.1 Concepto y evolución del metaverso 21

1.2 Características de los mundos virtuales 25

1.3 Tecnologías que sustentan el metaverso 31

1.4 Avatares e interacción virtual 36

1.5 Naturaleza jurídica del metaverso 41

1.6 Aplicación del derecho ecuatoriano en el metaverso 45

1.7 Vacíos y desafíos normativos 50

Capítulo 2 Identidad digital, privacidad y derechos fundamentales 53

2.1 Identidad digital y avatares 54

2.2 Datos personales y biométricos en el metaverso 58

2.3 Consentimiento y autodeterminación informativa 63

2.4 Intimidad, imagen y libertad de expresión 67

2.5 Protección de menores en el metaverso 71

2.6 Suplantación de identidad digital 76

2.7 Hábeas data y tutela digital 81

Capítulo 3 Capítulo 3 Economía virtual, propiedad digital y contratos inteligentes 87

3.1 Economía del metaverso 88

3.2 Bienes y activos digitales 90

3.3 Propiedad de bienes virtuales 93

3.4 NFT y activos digitales 97

3.5 Contratos electrónicos e inteligentes 100

3.6 Protección del consumidor virtual 104

3.7 Propiedad intelectual digital 109
3.8 Tributación de operaciones virtuales 114
Capítulo 4 Responsabilidad jurídica y delitos en entornos virtuales 119
4.1 Responsabilidad jurídica en el metaverso 120
4.2 Daños en entornos virtuales 124
4.3 Responsabilidad de las plataformas 128
4.4 Delitos en mundos virtuales 133
4.5 Acoso y violencia mediante avatares 138
4.6 Suplantación, fraude y activos digitales 143
4.7 Ciberseguridad en entornos inmersivos 147
4.8 Evidencia digital y jurisdicción 152
Capítulo 5 Gobernanza global y futuro de la regulación del metaverso 158
5.1 Soberanía y jurisdicción virtual 159
5.2 Gobernanza de las plataformas 163
5.3 Modelos de regulación del metaverso 168
5.4 Cooperación jurídica internacional 173
5.5 Derechos humanos y diseño tecnológico 179
5.6 Transparencia y responsabilidad algorítmica 184
5.7 Inclusión y sostenibilidad virtual 188
5.8 Regulación futura del metaverso en Ecuador 194
REFERENCIAS 198

Introducción

La expansión de los entornos digitales inmersivos está transformando la manera en que las personas construyen identidad, establecen relaciones, intercambian bienes, prestan servicios y participan en comunidades. Bajo la denominación de metaverso se agrupan plataformas persistentes e interactivas que integran realidad virtual y aumentada, inteligencia artificial, sensores, avatares, sistemas de identidad, cadenas de bloques y mecanismos de intercambio. Su relevancia jurídica no procede únicamente de la novedad tecnológica, sino de su capacidad para producir efectos personales, económicos y sociales que trascienden la sesión digital y se proyectan sobre sujetos jurídicamente identificables.

El metaverso no constituye una tecnología única ni un universo digital completamente integrado. En su estado actual, se manifiesta mediante ecosistemas diversos, administrados por empresas, comunidades, desarrolladores y proveedores de infraestructura que ofrecen distintos niveles de inmersión, persistencia, interoperabilidad y participación. Algunas plataformas se orientan al entretenimiento, mientras otras incorporan actividades educativas, laborales, comerciales, culturales o profesionales. Esta diversidad impide adoptar una definición excesivamente rígida y exige analizar las funciones concretas de cada entorno, los actores que intervienen, las tecnologías utilizadas y los riesgos jurídicos derivados de su funcionamiento.

La incorporación de avatares, sensores corporales, seguimiento ocular, reconocimiento de voz y sistemas de personalización amplía las posibilidades de interacción, pero también incrementa la recopilación de información personal. Las plataformas pueden observar movimientos, relaciones, preferencias, reacciones y comportamientos capaces de identificar al usuario o generar inferencias sobre su estado emocional, intereses y vulnerabilidades. La inmersión, por tanto, no representa solamente una mejora de la experiencia, sino una forma intensificada de tratamiento de datos. Esta característica plantea desafíos sobre consentimiento, autodeterminación informativa, biometría, intimidad, seguridad y decisiones automatizadas.

Los mundos virtuales también permiten desarrollar actividades económicas mediante monedas internas, bienes digitales, servicios, contenidos creados por usuarios, tokens y contratos inteligentes. Estas operaciones generan interrogantes sobre la naturaleza jurídica del activo adquirido, las facultades concedidas al usuario, la permanencia del

acceso y la relación entre control técnico, propiedad contractual y derechos intelectuales. La apariencia de posesión dentro de una plataforma no demuestra necesariamente la existencia de propiedad plena. Del mismo modo, la transferencia de un token no implica automáticamente la adquisición de la obra, el archivo o los derechos patrimoniales vinculados con él.

La persistencia de las cuentas, relaciones, contenidos y activos convierte a las plataformas en espacios capaces de concentrar intereses personales y patrimoniales relevantes. La suspensión de una cuenta, la modificación de reglas, la eliminación de un avatar o el cierre del servicio pueden afectar años de actividad, reputación, vínculos sociales, obras y recursos económicos. Los términos de servicio y los mecanismos de moderación no deben interpretarse como simples decisiones técnicas. Constituyen formas de gobernanza privada que distribuyen capacidades, imponen restricciones y condicionan el ejercicio efectivo de derechos dentro de los entornos virtuales.

La responsabilidad jurídica se vuelve especialmente compleja cuando en una misma interacción participan usuarios, operadores, desarrolladores, fabricantes de dispositivos, proveedores de nube, comerciantes, moderadores y agentes automatizados. Un daño puede originarse en una conducta humana, un error de programación, una falla de seguridad, una decisión algorítmica o una combinación de estos factores. La descentralización tampoco elimina la existencia de actores con capacidad de control, prevención o corrección. La imputación debe atender a las funciones efectivamente ejercidas, al riesgo creado, al beneficio obtenido y a la posibilidad real de evitar o limitar el perjuicio.

La dimensión transfronteriza añade dificultades relacionadas con jurisdicción, ley aplicable, cooperación institucional y ejecución de decisiones. Una interacción puede involucrar a un usuario residente en Ecuador, una empresa domiciliada en otro Estado, servidores distribuidos y activos registrados mediante redes descentralizadas. La ubicación física de un servidor no ofrece por sí sola una respuesta suficiente. Deben considerarse factores como residencia del usuario, mercado al que se dirige el servicio, lugar donde se manifiesta el daño, tratamiento de datos y control efectivo de la actividad. La protección jurídica requiere mecanismos nacionales e internacionales coordinados.

En Ecuador no existe una ley específica destinada exclusivamente al metaverso. Sin embargo, esto no significa que las actividades realizadas en mundos virtuales permanezcan fuera del ordenamiento. La Constitución de la República del Ecuador (2008), la LOPDP (2021), el Código Civil (2005), el COIP (2014), el COGEP (2015), la legislación de comercio electrónico, la normativa de consumo y el Código de la Niñez y Adolescencia (2003) permiten abordar numerosos conflictos. El desafío consiste en aplicar estas normas funcionalmente, identificar sus límites y determinar cuándo resultan necesarias reformas, reglamentos, estándares técnicos o mecanismos de cooperación.

Esta obra tiene como objetivo analizar los principales problemas jurídicos derivados de los mundos virtuales y establecer criterios para su tratamiento dentro del derecho ecuatoriano. Para ello, se adopta un enfoque jurídico, documental, analítico y propositivo basado en la revisión de normativa nacional, jurisprudencia constitucional y literatura científica de acceso abierto. El análisis no pretende presentar al metaverso como un territorio autónomo ni proponer una ley aislada para cada innovación. Su propósito es determinar cómo deben protegerse derechos, distribuirse responsabilidades y regularse actividades según sus funciones, riesgos y efectos concretos.

El libro se estructura en cinco capítulos. El primero examina los fundamentos tecnológicos, las características de los mundos virtuales, la naturaleza jurídica del metaverso y su relación con el derecho ecuatoriano. El segundo analiza identidad, privacidad, consentimiento, menores, suplantación y hábeas data. El tercero aborda economía, bienes digitales, propiedad, NFT, contratación, consumo, propiedad intelectual y tributación. El cuarto estudia responsabilidad, daños, plataformas, delitos, acoso, fraude, ciberseguridad y evidencia. El quinto desarrolla soberanía, gobernanza, modelos regulatorios, cooperación, derechos humanos, transparencia, inclusión y regulación futura en Ecuador.

La tesis central sostiene que el metaverso no constituye un espacio jurídicamente independiente, pero sus características inmersivas, persistentes, automatizadas y transfronterizas modifican las condiciones tradicionales de aplicación del derecho. Las normas vigentes ofrecen fundamentos importantes, aunque deben complementarse con obligaciones de diseño, transparencia, diligencia, evaluación de riesgos y cooperación internacional. Una regulación adecuada debe preservar la innovación sin convertirla en argumento para reducir derechos, ocultar responsabilidades o trasladar todos los riesgos

al usuario. La respuesta jurídica debe centrarse en los efectos reales y en la capacidad efectiva de cada actor para prevenirlos.

Capítulo 1

Fundamentos jurídicos y tecnológicos del metaverso

Andrea Mercedes Cedeño Cedeño



1.1 Concepto y evolución del metaverso

El metaverso puede entenderse como un ecosistema digital persistente, compartido e interactivo en el que las personas participan mediante avatares, crean contenidos y desarrollan actividades sociales, educativas, laborales y económicas. No constituye una única plataforma ni una tecnología aislada, sino la convergencia de infraestructuras, interfaces inmersivas, redes, sistemas de identidad, inteligencia artificial y mecanismos de intercambio. Su rasgo distintivo es la posibilidad de mantener relaciones y experiencias continuas dentro de espacios virtuales capaces de producir consecuencias más allá de la sesión tecnológica inmediata (Fernandez y Hui, 2022; Ghazinoory et al., 2025).

La literatura científica no ofrece una definición universalmente aceptada del metaverso. Algunas aproximaciones destacan la inmersión y la representación tridimensional, mientras otras priorizan la persistencia, la interoperabilidad, la presencia social, la economía digital o la producción de contenidos por los usuarios. Esta diversidad conceptual responde a que el fenómeno se encuentra en desarrollo y combina elementos tecnológicos, sociales y económicos. Jauhiainen et al. (2023) sostienen que su comprensión requiere analizar simultáneamente infraestructura, participación, sostenibilidad y gobernanza, evitando reducirlo a una experiencia de realidad virtual.

El metaverso tampoco debe confundirse con la realidad virtual. Esta última constituye una tecnología que puede proporcionar inmersión mediante visores, controladores y entornos generados informáticamente. El metaverso, en cambio, comprende también identidades digitales, relaciones entre usuarios, normas internas, actividades comerciales y mecanismos de creación compartida. Puede accederse a determinados mundos virtuales mediante computadoras, dispositivos móviles o realidad aumentada, sin utilizar necesariamente un visor. La inmersión favorece su desarrollo, pero no representa una condición única ni suficiente para definirlo (Song et al., 2023).

Los antecedentes conceptuales del metaverso se encuentran en la literatura de ciencia ficción, que imaginó espacios digitales habitables y paralelos al mundo físico. Estas narraciones describieron personas conectadas mediante representaciones virtuales, capaces de conversar, trabajar, adquirir bienes y recorrer escenarios informáticos. Aunque se trataba de formulaciones especulativas, anticiparon categorías que actualmente poseen relevancia tecnológica y jurídica, como avatar, presencia, identidad

virtual y economía digital. La evolución posterior trasladó gradualmente estas ideas desde la ficción hacia sistemas capaces de sostener interacciones reales entre comunidades conectadas (Kasiyanto y Kilinc, 2022).

Una primera etapa tecnológica estuvo representada por foros, chats, comunidades en línea y perfiles digitales. Estos espacios no ofrecían inmersión tridimensional, pero permitieron construir identidades, relaciones, reputaciones y reglas de convivencia en ambientes no físicos. Los usuarios comenzaron a experimentar formas de pertenencia y comunicación separadas de la proximidad territorial. Esta transformación demostró que las interacciones digitales podían producir efectos sociales y personales duraderos. También anticipó problemas relacionados con anonimato, privacidad, libertad de expresión y responsabilidad por contenidos generados dentro de comunidades virtuales (Fernandez y Hui, 2022).

Posteriormente, los videojuegos multijugador y los mundos virtuales persistentes ampliaron estas posibilidades. Los participantes comenzaron a controlar avatares, formar grupos, adquirir objetos y modificar espacios que continuaban existiendo después de su desconexión. La persistencia permitió que las acciones desarrolladas dentro de la plataforma produjeran consecuencias acumulativas, como reputación, relaciones, bienes virtuales y posiciones dentro de una comunidad. Jauhiainen et al. (2023) señalan que esta continuidad convirtió los mundos virtuales en espacios sociales y económicos, y no únicamente en experiencias recreativas limitadas a una partida.

El desarrollo de plataformas tridimensionales permitió que los usuarios dejaran de ser consumidores pasivos y comenzaran a crear escenarios, objetos, prendas, actividades y servicios. La producción participativa modificó la estructura de los mundos virtuales, porque el valor del entorno pasó a depender también de las contribuciones de su comunidad. Esta transformación generó nuevas oportunidades económicas y creativas, pero introdujo interrogantes sobre autoría, licencias, propiedad y distribución de beneficios. Jauhiainen et al. (2023) destacan que la creación participativa constituye una dimensión central de los ecosistemas virtuales y de sus modelos económicos.

La expansión de dispositivos de realidad virtual, sensores de movimiento y sistemas de seguimiento corporal intensificó la sensación de presencia. Los movimientos de la cabeza, las manos, la mirada y la voz pudieron trasladarse al entorno en tiempo real, haciendo que la interacción resultara más expresiva. Esta evolución incrementó las

posibilidades de educación, colaboración, entretenimiento y simulación. Al mismo tiempo, amplió la recopilación de información corporal y conductual, pues la experiencia comenzó a depender del registro continuo de señales capaces de identificar al usuario o revelar determinados aspectos de su comportamiento (Tukur et al., 2023).

Tabla 1
Evolución del metaverso y transformación de su relevancia jurídica

Etapa	Desarrollo predominante	Cambio en la experiencia	Implicación jurídica principal
Comunidades digitales iniciales	Foros, chats y perfiles	Comunicación e identidad a distancia	Privacidad, expresión y responsabilidad
Mundos persistentes	Videojuegos multijugador y avatares	Continuidad de relaciones y reputación	Conducta, daños y reglas privadas
Creación participativa	Objetos y espacios producidos por usuarios	Producción y comercialización de contenidos	Autoría, licencias y distribución de beneficios
Inmersión tecnológica	Realidad virtual, aumentada y sensores	Presencia corporal y participación sensorial	Datos personales, intimidad y seguridad
Economía virtual	Monedas internas, servicios y activos	Intercambio de valor dentro de plataformas	Contratación, consumo y propiedad
Descentralización	Cadena de bloques y registros distribuidos	Transferencia y trazabilidad de activos	Titularidad, fraude y jurisdicción
Ecosistemas inteligentes	Inteligencia artificial y automatización	Personalización y agentes virtuales	Transparencia, control y responsabilidad
Interoperabilidad emergente	Estándares y conexión entre plataformas	Traslado de datos, identidades y activos	Portabilidad y reconocimiento de derechos

Nota. Las etapas no son completamente sucesivas, pues varias tecnologías y modelos continúan coexistiendo dentro de los actuales entornos virtuales.

La realidad aumentada contribuyó a disminuir la separación entre los espacios físicos y digitales. En lugar de sustituir completamente el entorno material, incorpora objetos, imágenes e información virtual sobre lugares reales. Esta integración permite aplicaciones educativas, comerciales, médicas y productivas, pero también demuestra que el metaverso no debe concebirse exclusivamente como un universo desconectado. Ghazinoory et al. (2025) explican que las tecnologías inmersivas forman un continuo de experiencias con distintos grados de virtualidad, interacción y conexión con el espacio físico.

La cadena de bloques y los sistemas distribuidos constituyeron otra etapa relevante de esta evolución. Estas tecnologías permitieron registrar operaciones, emitir tokens y documentar transferencias sin depender exclusivamente de una base centralizada. Sin embargo, la descentralización no es un requisito indispensable para que exista un metaverso. Muchos mundos virtuales continúan siendo administrados por empresas que controlan servidores, cuentas, reglas y activos. Kasiyanto y Kilinc (2022) advierten que los registros distribuidos no eliminan la necesidad de identificar responsables ni garantizan automáticamente la legitimidad de las operaciones.

La inteligencia artificial ha ampliado las capacidades funcionales de los mundos virtuales. Puede emplearse para generar escenarios, adaptar experiencias, reconocer movimientos, traducir comunicaciones y crear personajes capaces de responder a los usuarios. También puede organizar contenidos y apoyar determinadas tareas de moderación. No obstante, la evolución hacia entornos automatizados introduce problemas relacionados con información, transparencia y control. El sistema puede influir en lo que cada persona observa o experimenta, de modo que las decisiones tecnológicas dejan de ser meramente operativas y adquieren consecuencias sociales y jurídicas (Ghazinoory et al., 2025; Küsters, 2026).

La interoperabilidad representa una de las aspiraciones más importantes del desarrollo actual. Consiste en permitir que identidades, objetos, credenciales o datos puedan trasladarse entre diferentes entornos. Sin embargo, esta capacidad continúa limitada por incompatibilidades técnicas, intereses comerciales y condiciones jurídicas distintas. Tukur et al. (2023) señalan que la transferencia de información entre plataformas amplía los riesgos de seguridad y privacidad. Además, trasladar técnicamente un objeto no significa que el nuevo entorno reconozca idénticas facultades de uso, modificación, comercialización o titularidad.

En su estado actual, el metaverso no constituye un universo único, integrado y plenamente interoperable. Existen múltiples plataformas con diferentes modelos de acceso, comunidades, economías y sistemas de gobernanza. Algunas ofrecen experiencias inmersivas, mientras otras funcionan mediante pantallas convencionales o combinan elementos físicos y virtuales. Resulta más preciso hablar de ecosistemas virtuales en proceso de integración. Jauhiainen et al. (2023) destacan que esta fragmentación condiciona la participación y dificulta establecer estándares comunes sobre identidad, sostenibilidad, acceso y administración de los entornos.

Desde el punto de vista jurídico, la novedad del metaverso no radica en que todas las conductas desarrolladas en él sean desconocidas para el derecho. Muchas actividades virtuales pueden relacionarse con categorías existentes de contratación, responsabilidad, protección de datos, propiedad intelectual o consumo. La dificultad surge porque la inmersión, la automatización, la persistencia y el carácter transfronterizo modifican las condiciones tradicionales de aplicación. Kostenko et al. (2022) sostienen que el reto consiste en adaptar los mecanismos jurídicos sin asumir que cada innovación tecnológica exige necesariamente un régimen completamente independiente.

En Ecuador no existe una ley dedicada exclusivamente al metaverso, pero estos entornos permanecen sometidos al ordenamiento cuando sus actividades producen efectos sobre personas, bienes o relaciones vinculadas con el país. La Constitución de la República del Ecuador (2008) aporta el marco general de derechos, mientras la legislación sectorial permite atender datos, contratación, consumo, propiedad intelectual y responsabilidad. La ausencia de una ley especial exige interpretación funcional y coordinación institucional, no la creación de un espacio inmune al derecho.

La evolución del metaverso demuestra el tránsito desde espacios digitales principalmente comunicativos hacia ecosistemas capaces de sostener identidades, economías, relaciones y actividades institucionales complejas. Su desarrollo no depende de una sola tecnología, sino de la interacción entre redes, interfaces, plataformas, inteligencia artificial y sistemas de intercambio. Esta convergencia explica por qué su estudio requiere perspectivas tecnológicas, sociales y jurídicas. Comprender su concepto y transformación histórica permite evitar definiciones rígidas y establecer una base coherente para analizar los derechos, riesgos y responsabilidades que surgen en los mundos virtuales (Fernandez y Hui, 2022).

1.2 Características de los mundos virtuales

Los mundos virtuales son entornos digitales compartidos en los que las personas pueden comunicarse, desplazarse, crear contenidos y participar mediante representaciones gráficas. Su identificación no depende únicamente de la utilización de imágenes tridimensionales o visores de realidad virtual. Lo que los distingue es la combinación de persistencia, interactividad, presencia social, participación colectiva, personalización y continuidad. Estas propiedades permiten que las acciones realizadas

dentro del entorno produzcan efectos duraderos sobre relaciones, reputación, contenidos y actividades económicas, diferenciándolos de aplicaciones digitales limitadas a una experiencia individual o temporal (Jauhiainen et al., 2023).

La persistencia constituye una característica central porque permite que el entorno continúe funcionando después de que un usuario finaliza su sesión. Los objetos creados, las modificaciones de los espacios, las relaciones establecidas y determinadas posiciones obtenidas permanecen disponibles para futuras interacciones. Esta continuidad facilita la formación de comunidades y economías estables. También genera expectativas respecto de la conservación de bienes, perfiles y contenidos. Fernandez y Hui (2022) señalan que la persistencia incrementa la cantidad de información acumulada sobre los participantes y amplía los riesgos vinculados con seguimiento y privacidad.

La persistencia no significa que los elementos virtuales sean permanentes o independientes del proveedor. Una plataforma puede modificar sus funciones, actualizar sus reglas, retirar objetos o cerrar definitivamente el servicio. La continuidad del mundo virtual suele depender de decisiones técnicas y empresariales. Esta situación produce una tensión entre las expectativas del usuario y las facultades contractuales del operador. Jauhiainen et al. (2023) advierten que el control estructural de las plataformas influye directamente en la autonomía de los participantes y en la estabilidad de las experiencias acumuladas.

La interactividad permite que los usuarios actúen sobre el espacio digital y reciban respuestas inmediatas del sistema o de otros participantes. La persona puede manipular objetos, modificar escenarios, conversar, colaborar o competir dentro del mismo entorno. Esta capacidad convierte al mundo virtual en un espacio dinámico y no en una representación pasiva. Song et al. (2023) explican que la interacción en tiempo real fortalece la sensación de participación y permite desarrollar experiencias sociales complejas. Al mismo tiempo, facilita conflictos, engaños y conductas capaces de producir consecuencias sobre terceros.

La presencia se refiere a la percepción psicológica de encontrarse dentro del entorno virtual y compartir un espacio con otros participantes. Puede fortalecerse mediante gráficos tridimensionales, sonido espacial, seguimiento corporal y respuesta inmediata del sistema. Una mayor sensación de presencia puede mejorar la colaboración, la

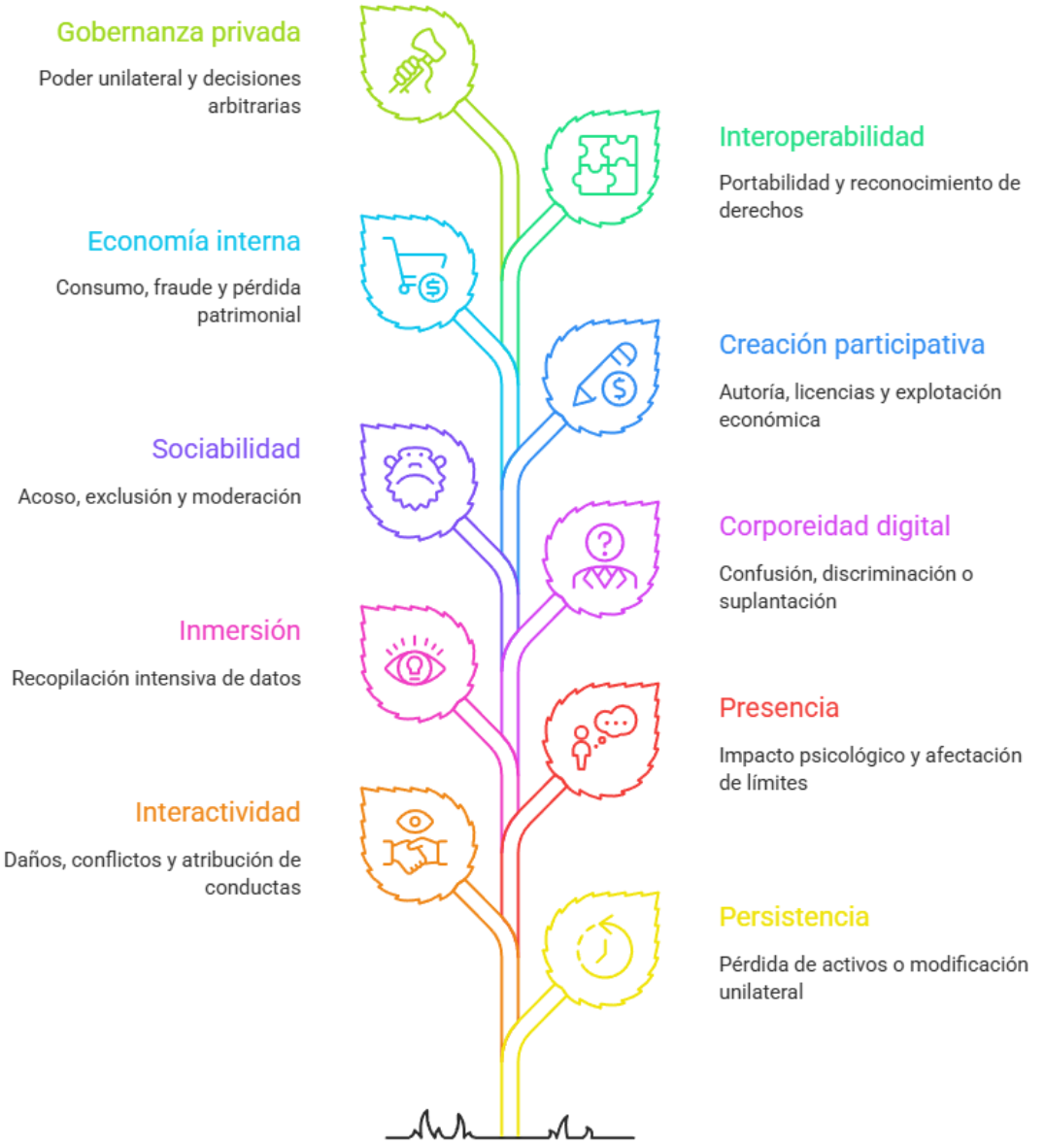
formación y el entretenimiento. Sin embargo, también puede intensificar el efecto emocional de amenazas, persecuciones o contactos invasivos. Munn y Weijers (2023) sostienen que la experiencia subjetiva del usuario debe considerarse al analizar los daños producidos dentro de escenarios inmersivos.

La inmersión describe el grado en que la tecnología concentra los sentidos y la atención de la persona en el entorno digital. Puede lograrse mediante visores, controladores, dispositivos hápticos o pantallas convencionales, aunque su intensidad varía según la infraestructura utilizada. No todos los mundos virtuales son completamente inmersivos ni requieren equipos especializados. Song et al. (2023) destacan que una mayor integración sensorial implica también una mayor recopilación de información corporal, pues el funcionamiento depende del registro de movimientos, voz, posición y otras señales asociadas con el usuario.

La corporeidad digital se manifiesta principalmente mediante el avatar, que proporciona una representación visible y operativa dentro del entorno. A través de él, la persona ocupa una posición, ejecuta acciones y se presenta ante los demás. El avatar puede reproducir rasgos reales, adoptar características ficticias o combinar elementos físicos e imaginarios. Esta libertad favorece creatividad y autorrepresentación, pero también puede producir confusión sobre identidad y autenticidad. En este capítulo, la corporeidad se aborda como característica funcional, mientras su protección jurídica detallada corresponde al capítulo dedicado a identidad digital.

La dimensión social permite que varias personas formen comunidades, establezcan vínculos y participen en actividades colectivas. Los mundos virtuales pueden albergar reuniones, clases, eventos, espacios de trabajo y experiencias recreativas. Estas relaciones no desaparecen necesariamente al desconectarse, pues pueden continuar en otras plataformas o trasladarse al ámbito físico. Jauhiainen et al. (2023) señalan que la sociabilidad constituye un componente esencial del metaverso, debido a que el valor de estos entornos depende de la participación, el reconocimiento mutuo y la construcción de prácticas compartidas.

Figura 1
Riesgos jurídicos en entornos virtuales



Nota. La figura resume los riesgos jurídicos vinculados con la gobernanza, la economía, la identidad, la interacción y la protección de derechos en entornos virtuales. Elaboración propia.

La simultaneidad permite que usuarios ubicados en distintos lugares participen en una misma actividad en tiempo real. Reuniones, conciertos, negociaciones o clases pueden desarrollarse con asistentes pertenecientes a diversas jurisdicciones. Esta característica crea una experiencia compartida, pero dificulta determinar dónde ocurrió jurídicamente una conducta. Song et al. (2023) explican que la sincronización constituye un elemento relevante para la sensación de copresencia. Desde el derecho, su importancia aparece cuando una interacción produce efectos simultáneos sobre personas, bienes o relaciones localizadas en diferentes países.

La creación participativa permite que los usuarios diseñen objetos, prendas, escenarios, obras y servicios. Esta facultad transforma al participante en productor y contribuye al crecimiento del entorno. Los mundos virtuales pueden depender significativamente de los contenidos generados por sus propias comunidades. Jauhiainen et al. (2023) señalan que esta participación amplía las oportunidades de creación y circulación de valor. La característica debe distinguirse de la propiedad sobre la infraestructura, pues el usuario puede producir contenidos dentro de una plataforma sin adquirir control sobre el sistema que los almacena.

La existencia de economías internas constituye otra característica relevante. Algunos mundos virtuales permiten comprar bienes, contratar servicios, intercambiar monedas internas o recibir remuneraciones por actividades realizadas. Estos elementos pueden adquirir valor por su utilidad, escasez, reconocimiento social o posibilidad de transferencia. Sin embargo, el valor económico no determina automáticamente que exista propiedad plena. Madanchian y Taherdoost (2024) advierte que los activos digitales pueden estar sometidos a condiciones contractuales, sistemas cerrados y mecanismos técnicos que limitan su utilización fuera de la plataforma.

La interoperabilidad consiste en la posibilidad de trasladar datos, identidades, objetos o credenciales entre distintos sistemas. Aunque suele presentarse como una característica esencial del futuro metaverso, todavía se encuentra limitada. Muchas plataformas utilizan formatos propios y no reconocen elementos generados externamente. Tukur et al. (2023) señalan que la interoperabilidad aumenta los riesgos de seguridad y privacidad debido al intercambio constante de información. Además, la compatibilidad técnica no garantiza que las distintas plataformas reconozcan las mismas licencias, condiciones de uso o facultades patrimoniales.

Los mundos virtuales pueden ser centralizados, descentralizados o combinar ambos modelos. En una plataforma centralizada, una empresa administra servidores, cuentas, contenidos y reglas. En sistemas descentralizados, determinadas funciones pueden distribuirse mediante protocolos o registros compartidos. Sin embargo, la utilización de cadena de bloques no elimina necesariamente la existencia de actores con capacidad de control. Ghazinoory et al. (2025) destacan que incluso los modelos descentralizados dependen de desarrolladores, interfaces y comunidades que adoptan decisiones. La estructura tecnológica influye en la identificación de responsabilidades.

La gobernanza privada se expresa mediante términos de servicio, códigos comunitarios, mecanismos de moderación y decisiones sobre acceso. Estas reglas determinan qué conductas están permitidas, qué contenidos pueden retirarse y bajo qué condiciones se suspende una cuenta. La gobernanza resulta necesaria para organizar comunidades numerosas, pero otorga a las plataformas un poder considerable sobre la expresión, la identidad y los intereses económicos de los usuarios. Munn y Weijers (2023) advierten que el diseño de los entornos virtuales condiciona la autonomía y las posibilidades reales de actuación. Las reglas internas deben ser transparentes, proporcionales y compatibles con los derechos aplicables.

La personalización permite adaptar avatares, contenidos, espacios y recomendaciones a las preferencias del usuario. Esta característica puede mejorar accesibilidad, creatividad y sentido de pertenencia. Sin embargo, suele apoyarse en la observación de decisiones, movimientos y relaciones. Fernandez y Hui (2022) señalan que la personalización intensiva puede convertirse en vigilancia cuando la plataforma recopila información más allá de lo necesario.

La escalabilidad determina la capacidad del sistema para aumentar usuarios, espacios y actividades sin perder funcionamiento. Un entorno con millones de participantes necesita infraestructura, moderación y seguridad diferentes de las requeridas por una comunidad pequeña. Chow et al. (2023) explican que el crecimiento de los mundos virtuales amplía la superficie de exposición y dificulta administrar incidentes. Las plataformas suelen recurrir a sistemas automatizados para gestionar grandes volúmenes de interacción, lo que puede mejorar la respuesta, pero también generar errores y decisiones carentes de suficiente contexto.

La accesibilidad condiciona quiénes pueden participar efectivamente. El costo de los dispositivos, la conectividad, el idioma y las adaptaciones funcionales influyen en el acceso real y pueden reproducir desigualdades preexistentes (Jauhiainen et al., 2023). En un ámbito más específico, Berrezueta et al. (2025) identifican oportunidades y barreras relacionadas con subtítulos, reconocimiento gestual, avatares y personalización para personas sordas. La accesibilidad debe incorporarse como característica estructural, probarse con usuarios diversos y mantenerse durante las actualizaciones.

Los mundos virtuales combinan continuidad tecnológica y consecuencias humanas. La persistencia, interactividad, inmersión, sociabilidad y economía interna permiten

construir experiencias que superan el uso individual y temporal de una aplicación. Estas propiedades modifican la manera en que se ejercen derechos, se forman expectativas y se distribuyen riesgos. Identificarlas permite comprender cómo el diseño asigna capacidades de actuación y control entre usuarios, plataformas y proveedores, sin confundir las características técnicas con una calificación jurídica automática (Song et al., 2023).

1.3 Tecnologías que sustentan el metaverso

El metaverso se construye mediante la integración de diversas tecnologías capaces de sostener entornos persistentes, interactivos, inmersivos y compartidos. No depende de un único dispositivo ni puede reducirse a la realidad virtual. Su funcionamiento requiere redes de comunicación, motores gráficos, sistemas de almacenamiento, sensores, inteligencia artificial, mecanismos de autenticación y herramientas de ciberseguridad. La combinación de estos componentes permite que numerosos usuarios participen simultáneamente, creen contenidos y desarrollen actividades sociales o económicas dentro de espacios digitales complejos (Song et al., 2023; Tukur et al., 2023).

La convergencia tecnológica constituye una característica estructural del metaverso. Cada componente cumple una función diferenciada, pero su utilidad aumenta cuando opera coordinadamente con los demás. Un visor puede proporcionar inmersión, aunque necesita conectividad, procesamiento gráfico y software para representar el entorno. Del mismo modo, un mundo virtual puede incorporar inteligencia artificial sin utilizar cadena de bloques. Esta interdependencia dificulta atribuir el funcionamiento completo de la plataforma a una sola herramienta y obliga a identificar qué actores desarrollan, administran y controlan cada capa tecnológica (Chow et al., 2023).

La realidad virtual permite situar perceptivamente al usuario dentro de un escenario generado mediante sistemas informáticos. A través de visores, controladores y sensores, la persona puede observar espacios tridimensionales, desplazarse y manipular objetos. La sensación de presencia surge cuando las respuestas visuales y auditivas se coordinan con los movimientos del cuerpo. Sin embargo, la realidad virtual constituye una vía de acceso y no el metaverso en su totalidad, porque este también comprende relaciones sociales, identidades, actividades económicas, contenidos y estructuras de gobernanza (Song et al., 2023).

La realidad aumentada incorpora información, imágenes u objetos digitales sobre el entorno físico. A diferencia de la realidad virtual, no sustituye completamente el espacio material, sino que añade capas informativas a lo que la persona observa. Puede utilizarse en educación, medicina, comercio, turismo y procesos productivos. Su relevancia para el metaverso radica en que conecta experiencias físicas y virtuales. Esta integración también introduce riesgos cuando la información digital altera la comprensión de espacios reales o dirige decisiones mediante datos incompletos, imprecisos o manipulados (Tukur et al., 2023).

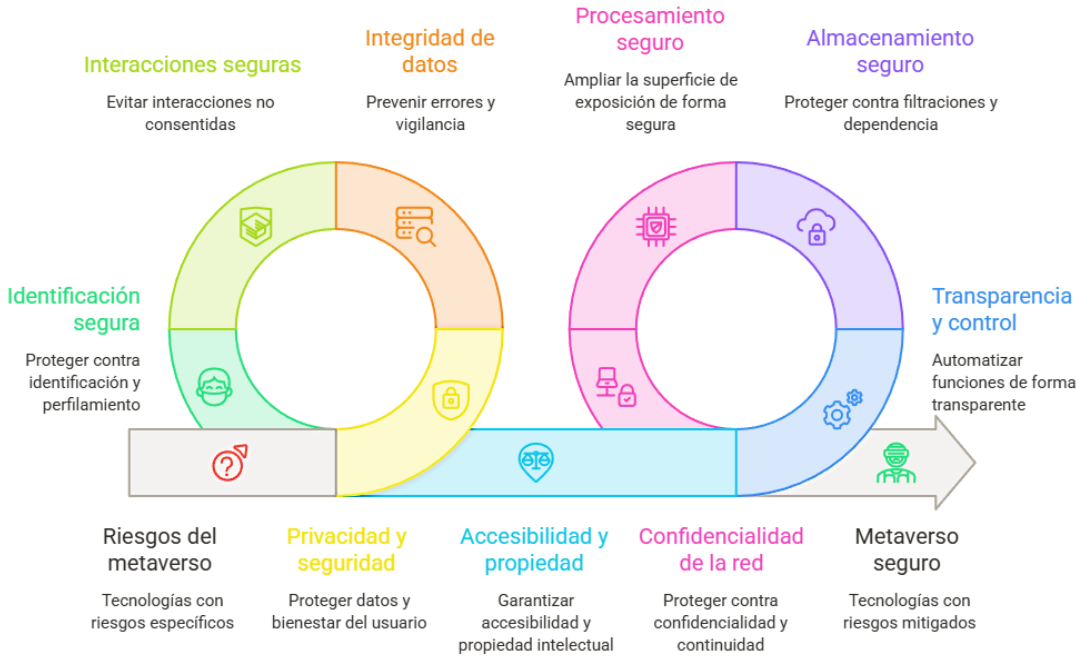
La realidad mixta profundiza esta integración al permitir que elementos físicos y virtuales interactúen entre sí. Un objeto digital puede permanecer asociado con una superficie real, responder al movimiento del usuario o modificar su comportamiento según información captada por sensores. Esta capacidad favorece simulaciones, actividades colaborativas y tareas profesionales. Sin embargo, los errores de posicionamiento, actualización o reconocimiento pueden generar decisiones equivocadas. La seguridad de estas experiencias depende de la precisión del sistema, la calidad de los datos y la coordinación entre dispositivos, aplicaciones y proveedores (Song et al., 2023).

Los dispositivos hápticos buscan incorporar sensaciones táctiles a los entornos inmersivos. Guantes, chalecos, controladores y otras interfaces pueden generar vibración, presión o resistencia para simular contacto con objetos o personas virtuales. Estas tecnologías aumentan el realismo y amplían las posibilidades de formación, rehabilitación y entretenimiento. Al mismo tiempo, intensifican la experiencia corporal del usuario y pueden convertir un evento digital en un estímulo físico. Munn y Weijers (2023) destacan que esta conexión sensorial obliga a considerar cuidadosamente límites, control personal y prevención de interacciones no deseadas.

Los sistemas de seguimiento corporal registran movimientos de cabeza, manos, rostro, ojos y otras partes del cuerpo para trasladarlos al avatar o al entorno. Esta información mejora la expresividad, la coordinación y la comunicación no verbal. También permite ejecutar actividades que requieren precisión motriz. No obstante, los patrones de movimiento pueden revelar características físicas, hábitos o condiciones particulares. Tukur et al. (2023) advierten que la recopilación constante de señales corporales amplía los riesgos de identificación, seguimiento y exposición de información sensible, especialmente cuando se conserva durante largos periodos.

Los motores gráficos constituyen la base informática para crear escenarios, objetos, iluminación, animaciones y efectos visuales. Procesan instrucciones y producen imágenes en tiempo real conforme a las acciones del usuario. También permiten que desarrolladores y participantes diseñen contenidos sin construir desde cero toda la infraestructura. Su importancia no es únicamente estética, porque la representación visual orienta la navegación, muestra advertencias, diferencia objetos y comunica reglas. Una interfaz gráfica confusa puede inducir errores, mientras un diseño claro puede mejorar seguridad, comprensión y accesibilidad (Song et al., 2023).

Figura 2
Mitigando los riesgos del metaverso



Nota. La figura presenta medidas orientadas a reducir los riesgos del metaverso mediante seguridad, privacidad, accesibilidad, transparencia, integridad y protección de los datos. Elaboración propia.

La inteligencia artificial cumple una función transversal dentro del metaverso: adapta experiencias, reconoce voz y movimientos, traduce comunicaciones, organiza contenidos y genera imágenes, objetos, voces, escenarios o respuestas de agentes virtuales. Ghazinoory et al. (2025) la identifican como una rama estructural de la arquitectura tecnológica del metaverso. Cuando estas capacidades se materializan en sistemas generativos o agentes autónomos, deben distinguirse los contenidos sintéticos, documentarse el origen de los datos y delimitarse las responsabilidades sobre los resultados. Küsters (2026) advierte, además, riesgos de manipulación, sesgo y colocación comercial encubierta.

La computación en la nube permite almacenar grandes volúmenes de información y ejecutar procesos en servidores remotos. Esta infraestructura facilita la sincronización de cuentas, la continuidad de los mundos virtuales y el acceso desde diferentes dispositivos. También permite ampliar la capacidad del sistema conforme aumenta el número de usuarios. No obstante, la concentración de datos en servicios externos incrementa el impacto potencial de una filtración o interrupción. Chow et al. (2023) señalan que la distribución de servicios requiere medidas coherentes de seguridad, disponibilidad y control de acceso.

La computación periférica o edge computing aproxima el procesamiento a los dispositivos o lugares donde se genera la información. Su finalidad es reducir la latencia y evitar que todos los datos deban viajar hacia servidores centrales distantes. Esta rapidez resulta importante en experiencias inmersivas, donde los retrasos pueden causar descoordinación o malestar. Sin embargo, distribuir el procesamiento entre múltiples nodos amplía la superficie de exposición. Chow et al. (2023) advierten que estos sistemas requieren controles consistentes para impedir accesos no autorizados y proteger la información procesada localmente.

Las redes de alta velocidad permiten transmitir imágenes, voz, movimientos y modificaciones del entorno con una demora reducida. La interacción simultánea exige que las acciones realizadas por un participante sean comunicadas rápidamente a los demás. Una latencia elevada puede afectar la coordinación y la sensación de presencia. La conectividad también genera metadatos sobre horarios, dispositivos y patrones de uso. Song et al. (2023) destacan que la infraestructura de comunicación es esencial para sostener experiencias compartidas, aunque sus desigualdades pueden limitar el acceso de comunidades con conectividad insuficiente.

La cadena de bloques permite registrar operaciones mediante bases distribuidas y mecanismos criptográficos. En algunos mundos virtuales se utiliza para emitir tokens, documentar transferencias o identificar el control técnico de determinados activos. Su trazabilidad puede aportar información sobre el historial de una operación, pero no garantiza por sí sola su legalidad. Kasiyanto y Kilinc (2022) advierten que una transacción registrada puede derivar de fraude, error o utilización indebida de credenciales. La inmutabilidad técnica tampoco resuelve automáticamente conflictos sobre nulidad, restitución o titularidad.

Los contratos inteligentes son programas que ejecutan instrucciones cuando se cumplen determinadas condiciones. Pueden facilitar pagos, transferencias y distribución automática de beneficios, pero su confiabilidad depende de la calidad del código, las fuentes externas de información y los mecanismos de verificación. Taherdoost (2023) identifica problemas persistentes de seguridad, escalabilidad, mantenimiento y vulnerabilidades de programación. La ejecución automática no sustituye el análisis de consentimiento, objeto, capacidad y responsabilidad, ni impide revisar resultados producidos por errores técnicos o credenciales utilizadas ilegítimamente.

El Internet de las cosas conecta sensores, dispositivos domésticos, vehículos y otros objetos físicos con servicios digitales. Dentro del metaverso, puede trasladar información del mundo material al entorno virtual o ejecutar acciones físicas a partir de instrucciones digitales. Esta conexión amplía las aplicaciones productivas y profesionales, pero también aumenta el alcance de los incidentes. Un ataque ya no se limitaría a alterar una representación informática, sino que podría afectar máquinas, edificios o actividades reales. Chow et al. (2023) destacan la necesidad de proteger cada dispositivo conectado y sus comunicaciones.

La identidad digital requiere sistemas de registro, autenticación y gestión de credenciales. Las plataformas pueden utilizar contraseñas, códigos temporales, certificados o biometría para verificar accesos. Cuanto mayor sea el valor social y económico de una cuenta, más graves serán las consecuencias de su apropiación. Fiaz et al. (2024) proponen estructuras de identidad autosoberana orientadas a fortalecer el control del usuario, reducir la exposición innecesaria de datos y mejorar la autenticación. Estas soluciones deben evaluarse conforme a proporcionalidad, accesibilidad, seguridad y posibilidad de recuperación.

La ciberseguridad atraviesa todas las capas tecnológicas del metaverso. Los riesgos pueden originarse en ataques externos, dispositivos comprometidos, aplicaciones defectuosas, permisos excesivos o errores humanos. La conexión entre identidades, sensores, comunicaciones y activos aumenta la superficie de exposición. Pooyandeh et al. (2022) describen amenazas relacionadas con accesos ilegítimos, manipulación de sistemas y vulnerabilidades de infraestructura. La protección debe integrar controles preventivos, detección de incidentes, recuperación de cuentas y actualización constante de los componentes tecnológicos utilizados.

El modelo de confianza cero, parte de la idea de que ninguna solicitud debe considerarse segura únicamente por proceder desde el interior de una red. Cada acceso debe verificarse según identidad, dispositivo, contexto y nivel de autorización. Gupta et al. (2023) relacionan este enfoque con control de accesos, segmentación y reducción de movimientos ilícitos dentro de la arquitectura del metaverso. Su aplicación debe ser proporcional, limitar la recopilación de datos y ofrecer mecanismos alternativos de autenticación cuando la biometría no resulte indispensable.

Las tecnologías que sostienen el metaverso no son neutrales, porque su diseño distribuye capacidades, riesgos y formas de control. La arquitectura determina qué información se recopila, qué acciones pueden realizarse, quién administra los activos y cómo se protegen los accesos. El análisis jurídico no debe concentrarse únicamente en las conductas visibles de los usuarios. También debe examinar la infraestructura, los modelos de negocio y las decisiones de quienes desarrollan, integran y administran estos sistemas, considerando las funciones específicas de cada componente tecnológico (Tukur et al., 2023).

1.4 Avatares e interacción virtual

Los avatares son representaciones digitales mediante las cuales las personas actúan dentro de los mundos virtuales. Pueden adoptar formas realistas, estilizadas, fantásticas o completamente abstractas y permiten desplazarse, comunicarse, manipular objetos y participar en actividades colectivas. Su función no se limita a mostrar una imagen, porque también organizan la presencia del usuario dentro del entorno. Mediante el avatar, la persona ocupa una posición reconocible, ejecuta acciones y establece relaciones con otros participantes o con sistemas automatizados (Munn y Weijers, 2023).

La apariencia del avatar puede construirse a partir de rasgos elegidos manualmente o de información captada mediante fotografías, escaneos y sensores. Algunas representaciones reproducen el rostro, la voz y los movimientos del usuario, mientras otras permiten adoptar características completamente diferentes. Esta flexibilidad favorece la creatividad, la experimentación y la participación en comunidades virtuales. No obstante, el avatar no debe confundirse con una identidad jurídica autónoma. Funciona como una interfaz de representación, pero las consecuencias de sus

actuaciones continúan vinculadas con personas, organizaciones o sistemas responsables (Song et al., 2023).

La personalización constituye una dimensión esencial de la experiencia virtual. Los usuarios pueden seleccionar nombre, vestimenta, accesorios, características corporales y formas de movimiento para expresar preferencias o pertenencia comunitaria. Estas decisiones contribuyen a construir una presencia reconocible dentro del entorno y pueden fortalecer el sentido de identificación con el avatar. Castillo et al. (2024) señalan que las herramientas de creación de avatares desempeñan un papel importante en la construcción de la identidad virtual, aunque también pueden recopilar información personal durante el proceso de configuración.

La interacción virtual comprende los actos comunicativos, corporales y espaciales desarrollados entre usuarios, avatares y agentes automatizados. Puede manifestarse mediante texto, voz, gestos, movimientos, proximidad, manipulación de objetos y reacciones del entorno. A diferencia de una comunicación basada únicamente en mensajes, los mundos virtuales combinan varias formas expresivas de manera simultánea. Esta riqueza permite experiencias más dinámicas, pero también introduce ambigüedades, porque una acción puede derivar de una decisión consciente, una respuesta automática, una limitación del dispositivo o un error técnico (Tukur et al., 2023).

La comunicación verbal conserva una función central dentro de los espacios inmersivos. Los usuarios pueden conversar en tiempo real, participar en reuniones, recibir instrucciones o coordinar actividades mediante voz y texto. La incorporación de herramientas de traducción facilita la interacción entre personas de distintas lenguas, aunque puede modificar el sentido de expresiones, tonos o referencias culturales. Cuando una conversación produce consecuencias relevantes, resulta necesario considerar el contexto, la identidad de los participantes y la fiabilidad de los sistemas utilizados para transmitir, registrar o traducir el contenido.

La comunicación no verbal adquiere especial relevancia cuando los sistemas reproducen mirada, postura, gestos y distancia corporal. Estas señales pueden expresar atención, rechazo, entusiasmo o incomodidad, pero no poseen un significado uniforme. Una misma conducta puede interpretarse de forma distinta según la cultura, la capacidad física o el contexto de la interacción. Además, el avatar puede ejecutar movimientos

corregidos o generados automáticamente por el sistema. No debe atribuirse intención jurídica a toda expresión virtual sin examinar previamente cómo fue producida y qué control conservaba el usuario.

La sensación de presencia intensifica el significado de la interacción. Cuando una persona percibe que comparte un espacio con otros participantes, las conversaciones, aproximaciones y movimientos pueden generar respuestas emocionales más fuertes que en medios menos inmersivos. Munn y Weijers (2023) explican que los mundos virtuales pueden producir experiencias psicológicamente significativas, incluso cuando los cuerpos no se encuentran físicamente próximos. Esta característica permite desarrollar actividades educativas, profesionales y recreativas, pero también exige reconocer que ciertas conductas virtuales pueden afectar de manera real el bienestar del usuario.

Los dispositivos hápticos profundizan la interacción al convertir determinados eventos digitales en estímulos físicos. Una acción realizada por otro avatar puede generar vibración, presión o resistencia sobre el cuerpo del usuario. Estas tecnologías amplían las posibilidades de simulación, entrenamiento y rehabilitación, pero también incrementan la necesidad de controles personales. La interacción sensorial debe poder configurarse, reducirse o interrumpirse de forma inmediata. El diseño tecnológico debe garantizar que la intensidad, duración y alcance del estímulo permanezcan bajo el control efectivo de quien utiliza el dispositivo (Tukur et al., 2023).

Tabla 2
Dimensiones funcionales de los avatares y la interacción virtual

Dimensión	**Manifestación dentro del entorno**	**Función principal**	**Riesgo predominante**
Representación visual	Apariencia, nombre y vestimenta	Identificación dentro de la comunidad	Confusión o copia no autorizada
Movimiento	Gestos, postura y desplazamiento	Expresión y navegación	Atribución incorrecta de acciones
Comunicación verbal	Voz, texto y traducción	Coordinación e intercambio	Distorsión del mensaje
Comunicación no verbal	Mirada, distancia y expresiones	Transmisión de señales sociales	Interpretación ambigua
Presencia	Sensación de compartir un espacio	Intensificación de la experiencia	Impacto emocional

Dimensión	Manifestación dentro del entorno	Función principal	Riesgo predominante
Interacción háptica	Vibración, presión y resistencia	Simulación de contacto	Estímulos no deseados
Personalización	Selección de rasgos y accesorios	Autorrepresentación	Recopilación excesiva de datos
Actuación automatizada	Respuestas generadas por el sistema	Continuidad y asistencia	Confusión entre persona y programa
Interacción económica	Compra, intercambio y uso de objetos	Participación comercial	Operaciones no comprendidas
Interacción institucional	Uso de cargos e insignias	Representación de organizaciones	Apariencia falsa de autoridad

Nota. Las dimensiones pueden combinarse dentro de una misma experiencia y no implican por sí solas una calificación jurídica determinada.

Los límites personales pueden incorporarse directamente en la arquitectura del entorno mediante zonas de distancia, bloqueo, silenciamiento y salida inmediata. Estas herramientas permiten que la persona controle la intensidad de la interacción y reduzca la dependencia de una intervención posterior. Sakka et al. (2026) sostienen que los límites digitales deben poder expresarse y modificarse durante la experiencia. Para ser efectivos, los controles deben resultar visibles, reversibles y accesibles, y mantenerse activos frente a nuevas funciones o actualizaciones.

Los avatares también pueden participar en actividades económicas mediante la compra de objetos, contratación de servicios o intercambio de activos. La interfaz debe diferenciar con claridad las acciones recreativas de aquellas que generan pagos, transferencias o compromisos. Un gesto, una orden verbal o la manipulación de un objeto solo debería producir consecuencias patrimoniales cuando el usuario haya recibido información suficiente y exista una confirmación inequívoca. Esta separación reduce errores y evita que la inmersión o la rapidez de la interacción oculten la naturaleza económica de la operación.

La interacción institucional se produce cuando un avatar representa a una empresa, universidad, organismo público o profesional. Uniformes, insignias, nombres y credenciales pueden facilitar el reconocimiento de funciones dentro del entorno. Sin embargo, la apariencia no demuestra por sí sola que la persona posea el cargo o autorización que afirma ejercer. Los sistemas deben permitir verificar representaciones institucionales cuando la interacción implique decisiones, asesoramiento o acceso a

servicios. Esta verificación adquiere importancia en reuniones, actividades educativas, atención al usuario y operaciones comerciales.

Los avatares pueden estar controlados total o parcialmente por inteligencia artificial. Algunos funcionan como asistentes, tutores, vendedores, personajes narrativos o moderadores. Su lenguaje y apariencia pueden aproximarse a los de una persona, especialmente cuando combinan reconocimiento de voz, generación de respuestas y animación corporal. Küsters (2026) advierte que estos agentes pueden generar confianza indebida, colocación comercial encubierta y manipulación cuando su naturaleza automatizada no se comunica claramente. En estos casos, la plataforma debe evitar que la similitud produzca confusión. El participante necesita conocer cuándo interactúa con un sistema automatizado, sobre todo si este solicita información, ofrece productos o influye en decisiones relevantes.

También existen avatares híbridos que combinan acciones humanas con funciones automáticas. El sistema puede corregir movimientos, completar expresiones, responder mensajes o mantener determinada actividad mientras el usuario se encuentra desconectado. Esta combinación mejora continuidad y accesibilidad, pero dificulta distinguir qué conducta provino directamente de la persona y cuál fue generada por el programa. Küsters (2026) subraya que la atribución se vuelve especialmente compleja cuando el agente conserva iniciativa o actúa durante la desconexión del usuario. La arquitectura debería permitir identificar la intervención de cada componente cuando sea necesario, sin almacenar de manera permanente todos los movimientos o conversaciones producidos durante la experiencia.

La interacción virtual puede generar dificultades técnicas que alteren la percepción de una conducta. Retrasos, fallos de seguimiento, errores de traducción, desconexiones y movimientos involuntarios pueden modificar la acción visible del avatar. Una aproximación invasiva podría originarse en un problema de control, mientras una respuesta aparentemente ofensiva podría deberse a una traducción defectuosa. Song et al. (2023) destacan que la complejidad de los entornos inmersivos amplía los puntos de fallo. La interpretación de las conductas debe considerar siempre las condiciones técnicas en las que ocurrieron.

La participación de personas con discapacidad depende de la configuración de los avatares, los dispositivos y las interfaces. Berrezueta et al. (2025) destacan el potencial

de la retroalimentación visual, el reconocimiento gestual, los avatares y los entornos adaptativos para apoyar a personas sordas o con dificultades auditivas, aunque advierten costos, limitaciones técnicas y ausencia de diseño inclusivo. Los sistemas deben ofrecer controles alternativos, subtítulos y personalización, evitando interpretar de manera uniforme movimientos, gestos o formas diversas de comunicación.

Los avatares y la interacción virtual conectan a la persona con el entorno digital y permiten presencia, comunicación, actuación y reconocimiento dentro de espacios compartidos. Su funcionamiento depende de decisiones sobre apariencia, movimiento, automatización, accesibilidad y control sensorial. Comprender estas funciones resulta indispensable para analizar posteriormente la identidad, el consentimiento, la responsabilidad y los daños, porque una misma acción visible puede proceder del usuario, del sistema o de una combinación de ambos (Munn y Weijers, 2023).

1.5 Naturaleza jurídica del metaverso

La naturaleza jurídica del metaverso no puede explicarse mediante una sola categoría, porque estos entornos integran infraestructura tecnológica, relaciones sociales, actividades económicas, tratamiento de datos y mecanismos privados de gobernanza. No constituyen únicamente programas informáticos ni espacios de entretenimiento, pues permiten contratar, crear contenidos, adquirir activos, organizar comunidades y producir daños. Kasiyanto y Kilinc (2022) sostienen que el análisis jurídico debe considerar simultáneamente la arquitectura tecnológica, los actores involucrados y los efectos generados. El metaverso posee una naturaleza compleja, funcional y multidimensional.

El metaverso tampoco constituye un territorio soberano separado de los Estados. Aunque reproduzca ciudades, oficinas, viviendas o espacios públicos, carece de territorio físico, población jurídicamente independiente y poder soberano originario. Las plataformas pueden establecer reglas internas, pero esas disposiciones no sustituyen las leyes nacionales ni los instrumentos internacionales. Kostenko et al. (2022) advierten que los mundos virtuales operan dentro de relaciones jurídicas preexistentes y continúan vinculados con jurisdicciones, empresas y usuarios localizables. La representación espacial no transforma al entorno digital en un nuevo Estado.

Desde una perspectiva tecnológica, el metaverso puede ser entendido como una plataforma o conjunto de plataformas que ofrecen servicios digitales. Esta calificación

permite identificar al operador, sus funciones y el grado de control que ejerce sobre servidores, cuentas, interfaces y contenidos. No todas las plataformas poseen la misma estructura, pues algunas concentran decisiones y otras distribuyen ciertas funciones mediante protocolos descentralizados. Sin embargo, incluso en modelos distribuidos deben reconocerse los actores que diseñan, mantienen o administran componentes esenciales del sistema (Kasiyanto y Kilinc, 2022).

El metaverso también funciona como espacio de interacción social. En él se forman comunidades, reputaciones, relaciones laborales, educativas y comerciales que pueden prolongarse fuera de la plataforma. Esta dimensión impide reducirlo a una infraestructura neutral. Jauhiainen et al. (2023) destacan que las reglas de diseño y moderación influyen en la autonomía, la participación y la experiencia de los usuarios. La plataforma no solo aloja contenidos, sino que organiza conductas, distribuye visibilidad y determina qué acciones son técnicamente posibles dentro del entorno.

Desde el punto de vista económico, el metaverso opera como mercado digital. Los participantes pueden comprar objetos, contratar servicios, crear obras, asistir a eventos y recibir remuneraciones. Estas actividades pueden generar derechos personales, licencias, saldos contractuales o intereses patrimoniales, aunque no toda adquisición equivalga a propiedad plena. Jauhiainen et al. (2023) señalan que la economía virtual combina creación participativa, consumo y circulación de valor. Su naturaleza jurídica debe determinarse según la función real de cada operación y no únicamente por la denominación comercial empleada.

El metaverso constituye igualmente un ecosistema intensivo de datos. Para funcionar puede recopilar información identificativa, técnica, corporal, conductual y relacional. La identidad del usuario, sus movimientos, sus preferencias y sus interacciones pueden ser procesados por diferentes actores. Fernandez y Hui (2022) explican que los entornos inmersivos amplían la capacidad de observación y perfilamiento. Esta dimensión determina que la naturaleza jurídica del metaverso no dependa únicamente de contratos o activos, sino también del tratamiento de información y del control ejercido sobre la arquitectura digital.

La gobernanza privada representa otra dimensión fundamental. Los términos de servicio, códigos comunitarios y mecanismos de moderación determinan el acceso, la permanencia y las conductas permitidas. Estas reglas poseen eficacia contractual y

técnica, pero no equivalen a normas estatales. Kasiyanto y Kilinc (2022) explican que las plataformas ejercen poder regulatorio mediante contratos y arquitectura, aunque permanecen sometidas al derecho aplicable. La gobernanza interna debe examinarse como una forma de regulación privada subordinada a derechos fundamentales, normas imperativas y mecanismos externos de tutela.

El carácter híbrido del metaverso también deriva de la interacción entre espacios físicos y digitales. La realidad aumentada, los dispositivos hápticos y el Internet de las cosas pueden trasladar información o acciones entre ambas dimensiones. Una instrucción virtual puede afectar un dispositivo real, mientras un sensor físico puede modificar la representación digital. Song et al. (2023) destacan que el metaverso se desarrolla como un continuo entre lo material y lo virtual. Esta integración obliga a analizar los efectos concretos de cada conducta y evita tratar todos los acontecimientos como exclusivamente digitales.

Tabla 3
Dimensiones que integran la naturaleza jurídica del metaverso

Dimensión	**Manifestación principal**	**Relación jurídica predominante**	**Cuestión central**
Infraestructura tecnológica	Servidores, software, redes e interfaces	Prestación de servicios digitales	Control y seguridad del sistema
Espacio de interacción	Comunidades, reuniones y actividades sociales	Relaciones personales y organizativas	Conductas y protección de participantes
Mercado digital	Bienes, servicios, monedas y activos	Contratación y consumo	Naturaleza del derecho adquirido
Ecosistema de datos	Registro de identidad, movimientos y preferencias	Tratamiento de datos personales	Finalidad, seguridad y control
Entorno creativo	Obras, objetos y escenarios creados por usuarios	Autoría y licencias	Titularidad y explotación
Gobernanza privada	Términos, moderación y sanciones	Contrato de adhesión	Límites del poder de la plataforma
Sistema automatizado	Algoritmos y agentes virtuales	Decisiones y servicios automatizados	Transparencia y atribución
Entorno transfronterizo	Usuarios y proveedores en distintos países	Conflicto de leyes y jurisdicción	Norma y autoridad competente

Dimensión	Manifestación principal	Relación jurídica predominante	Cuestión central
Espacio híbrido	Conexión entre elementos físicos y digitales	Responsabilidad por efectos reales	Causalidad e imputación
Comunidad económica	Trabajo, creación y remuneración virtual	Actividad profesional y comercial	Derechos y obligaciones de participantes

Nota. Las dimensiones pueden coexistir dentro de una misma plataforma y requieren una calificación jurídica diferenciada según la actividad examinada.

El metaverso no posee personalidad jurídica propia. La plataforma puede pertenecer a una empresa, una organización o un conjunto de participantes, pero el entorno tecnológico no se convierte por ello en sujeto autónomo de derechos y obligaciones. Tampoco los avatares o agentes artificiales adquieren personalidad por actuar dentro del sistema. La responsabilidad debe dirigirse hacia las personas naturales o jurídicas que controlan, diseñan, utilizan o se benefician de la actividad. Kostenko et al. (2022) destacan la necesidad de identificar actores y funciones reales.

La relación entre plataforma y usuario suele tener naturaleza contractual. El acceso se encuentra condicionado por términos de servicio, políticas de privacidad y reglas comunitarias aceptadas mediante procedimientos electrónicos. Sin embargo, la existencia de un contrato no significa que todas sus cláusulas sean válidas ni que la empresa pueda modificar unilateralmente derechos esenciales. El Código Civil (2005) y la legislación de consumo permiten analizar consentimiento, objeto, obligaciones y cláusulas abusivas. El componente contractual constituye una dimensión del metaverso, pero no agota todas las relaciones jurídicas existentes.

Los objetos virtuales tampoco poseen una naturaleza jurídica uniforme. Un accesorio para avatar puede constituir una licencia de uso, una entrada virtual puede representar un derecho personal y una creación digital puede estar protegida por propiedad intelectual. En otros casos, el usuario únicamente obtiene acceso revocable a una función. Martínez et al. (2024) sostienen que el análisis debe diferenciar control técnico, titularidad contractual y derechos intelectuales. La apariencia de propiedad dentro de la interfaz no determina por sí sola el derecho jurídicamente adquirido.

La descentralización tecnológica no modifica automáticamente la naturaleza jurídica de una operación. La utilización de cadenas de bloques puede distribuir registros y reducir la dependencia de una base central, pero siempre existen personas que desarrollan

protocolos, administran interfaces o utilizan credenciales. Kasiyanto y Kilinc (2022) explican que la descentralización puede dificultar la identificación de responsables, aunque no elimina obligaciones jurídicas. Un sistema distribuido continúa sometido a reglas sobre contratación, fraude, protección de datos y responsabilidad cuando produce efectos sobre personas identificables.

La inteligencia artificial añade una dimensión automatizada a la naturaleza del metaverso. Los sistemas pueden generar contenidos, adaptar experiencias, administrar accesos o ejecutar decisiones sin intervención humana directa en cada caso. Sin embargo, la autonomía técnica no convierte al algoritmo en sujeto responsable. Deben identificarse las personas y organizaciones que lo desarrollan, implementan y supervisan. Ghazinoory et al. (2025) destacan la creciente integración de inteligencia artificial en entornos inmersivos, lo que exige distinguir entre funcionamiento automatizado, control empresarial y actuación del usuario.

En Ecuador, la calificación jurídica del metaverso debe construirse a partir de las categorías existentes y de los efectos reales de cada actividad. La Constitución de la República del Ecuador (2008) protege derechos que permanecen vigentes en entornos digitales, mientras la legislación civil, comercial, penal y de protección de datos permite abordar operaciones específicas. No resulta necesario considerar al metaverso como un ordenamiento autónomo. Lo importante es identificar la relación jurídica, los actores, el derecho comprometido y la norma aplicable en cada situación.

La naturaleza jurídica del metaverso es, por tanto, plural y variable. Puede funcionar simultáneamente como plataforma, mercado, comunidad, ecosistema de datos y espacio creativo. Ninguna categoría aislada explica todas sus relaciones. La calificación debe atender a la actividad concreta, al control ejercido por cada actor y a los efectos producidos. Este enfoque evita interpretaciones generales que confundan representación tecnológica con realidad jurídica y permite aplicar las normas existentes de manera funcional, sin negar la necesidad de ajustes frente a riesgos emergentes.

1.6 Aplicación del derecho ecuatoriano en el metaverso

El metaverso no constituye un espacio ajeno al ordenamiento jurídico ecuatoriano. Las actividades realizadas mediante avatares, plataformas inmersivas, sistemas automatizados o activos digitales pueden quedar sometidas a normas nacionales cuando involucren personas residentes en Ecuador, proveedores dirigidos al mercado

ecuatoriano o consecuencias producidas dentro del país. La ubicación técnica de los servidores no determina por sí sola el derecho aplicable. Deben considerarse los sujetos participantes, el lugar donde se manifiesta el daño, la finalidad del servicio y la conexión efectiva de la relación con Ecuador (Kostenko et al., 2022).

La aplicación jurídica debe partir de una interpretación funcional y no exclusivamente territorial. Una interacción puede involucrar a un usuario ecuatoriano, una empresa domiciliada en otro Estado, infraestructura distribuida y participantes ubicados en varios países. En estas circunstancias, localizar físicamente cada componente resulta insuficiente. Kasiyanto y Kilinc (2022) sostienen que los mundos virtuales intensifican los conflictos de jurisdicción porque combinan descentralización, anonimato y operaciones transfronterizas. La respuesta debe identificar qué ordenamiento posee una vinculación razonable con la actividad y qué autoridad puede ofrecer tutela efectiva.

La Constitución de la República del Ecuador (2008) proporciona el fundamento general para proteger derechos dentro de los entornos virtuales. La dignidad, igualdad, identidad, intimidad, libertad de expresión, propiedad y seguridad jurídica no desaparecen cuando la interacción se realiza mediante medios digitales. El artículo 11 establece la aplicación directa de los derechos y exige interpretar las normas de manera favorable a su vigencia. Esta disposición permite responder frente a vulneraciones tecnológicas incluso cuando la modalidad concreta no se encuentre descrita expresamente en una ley especializada.

La aplicación constitucional no implica trasladar automáticamente todas las categorías del espacio físico al metaverso. Una representación virtual no equivale necesariamente a una persona jurídica, un terreno digital no constituye un inmueble y una regla de plataforma no posee el valor de una ley estatal. Cada situación debe analizarse según su función y sus efectos. Kasiyanto y Kilinc (2022) advierten que la regulación de los mundos virtuales requiere evitar analogías simplificadoras que confundan el lenguaje comercial o tecnológico con la naturaleza jurídica real de las relaciones.

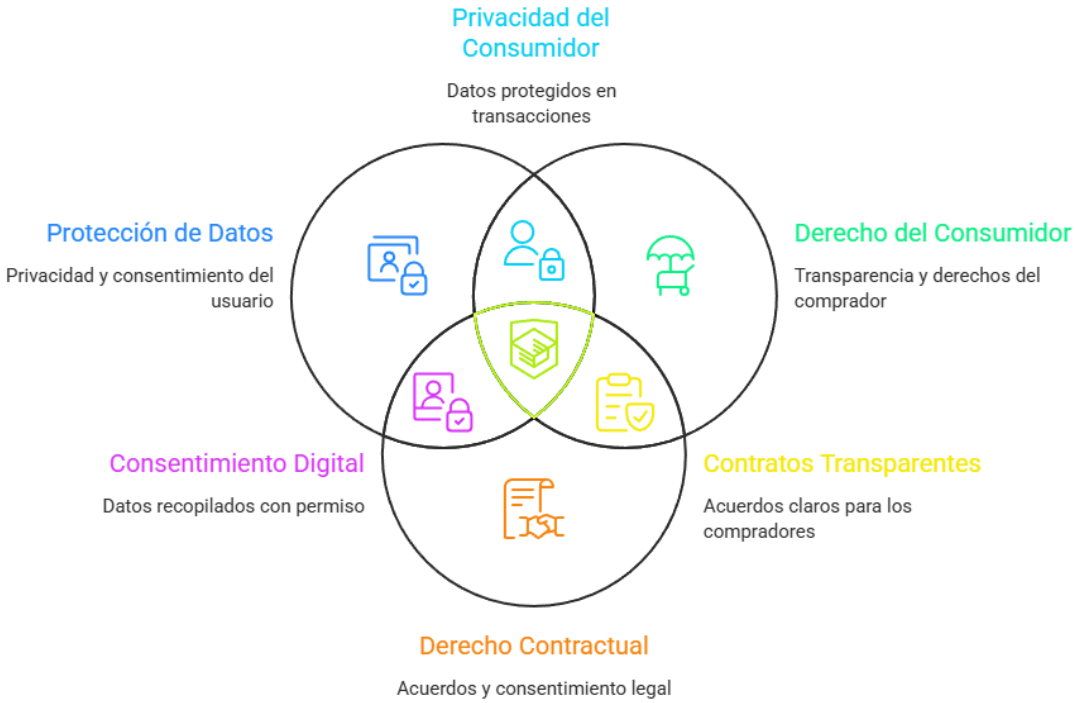
La protección de datos personales forma uno de los principales puntos de conexión con el derecho ecuatoriano. La LOPDP (2021), artículo 3, extiende su aplicación a determinados responsables no establecidos en Ecuador cuando ofrecen bienes o servicios a residentes o controlan su comportamiento. Esta regla puede comprender plataformas extranjeras que recopilan movimientos, voz, preferencias o interacciones

de usuarios ecuatorianos. Fernandez y Hui (2022) destacan que la observación continua en entornos inmersivos permite construir perfiles detallados, por lo que la aplicación territorial debe considerar el seguimiento efectivo de las personas.

La LOPDP (2021) también resulta aplicable cuando la información permite identificar directa o indirectamente a un usuario. El uso de un avatar, seudónimo o nombre ficticio no elimina la protección si la plataforma conserva direcciones electrónicas, dispositivos, credenciales o registros capaces de vincular la actividad con una persona. Tukur et al. (2023) señalan que los entornos inmersivos combinan múltiples señales técnicas y conductuales, aumentando las posibilidades de reidentificación. La aplicación de la ley depende del tratamiento realizado y no únicamente de la información visible para otros participantes.

Las relaciones contractuales desarrolladas dentro del metaverso pueden someterse al Código Civil (2005) y a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002). La utilización de una interfaz inmersiva no impide que exista consentimiento, siempre que la persona comprenda la operación y exteriorice su voluntad. Los mensajes de datos pueden producir efectos jurídicos equivalentes a los documentos tradicionales. Sin embargo, un movimiento, gesto o contacto con un objeto digital no constituye automáticamente aceptación si la plataforma no informa claramente sus consecuencias económicas o contractuales.

Figura 3
Intersecciones Legales en el Metaverso Ecuatoriano



Nota. La figura representa la relación entre protección de datos, derecho del consumidor y derecho contractual en el metaverso ecuatoriano, destacando la privacidad, el consentimiento y la transparencia. Elaboración propia.

La legislación de protección al consumidor puede aplicarse cuando una plataforma ofrece bienes o servicios a personas ubicadas en Ecuador. La Ley Orgánica de Defensa del Consumidor (2000) exige información clara, trato transparente y protección frente a cláusulas abusivas. Estas obligaciones comprenden precios, duración, funcionalidad, restricciones de transferencia y condiciones de pérdida de activos. La apariencia inmersiva o el uso de monedas internas no debe ocultar el valor real de la operación. El proveedor continúa obligado a responder por información engañosa o servicios defectuosos.

Las cláusulas de elección de ley o jurisdicción incluidas en términos de servicio no siempre desplazan las normas imperativas ecuatorianas. Una plataforma puede establecer que sus contratos se rijan por una legislación extranjera, pero esta disposición no debería eliminar derechos mínimos del consumidor ni impedir el acceso a mecanismos de tutela. Kostenko et al. (2022) explican que las plataformas globales intentan uniformar sus relaciones mediante contratos de adhesión, aunque los Estados conservan la facultad de aplicar normas protectoras cuando el servicio se dirige a sus residentes.

La aplicación del derecho penal exige una conexión territorial y la correspondencia exacta entre la conducta y un tipo previsto en el COIP (2014). La existencia de un daño virtual no permite crear delitos mediante analogía. Pueden resultar aplicables normas sobre estafa, apropiación fraudulenta por medios electrónicos, interceptación ilegal de datos, ataques contra sistemas y acceso no consentido. Varela et al. (2025) destacan que la inteligencia artificial y las identidades sintéticas amplían las modalidades de ciberdelincuencia, pero la imputación continúa requiriendo autoría, intención y evidencia suficiente.

La atribución de una conducta realizada mediante un avatar requiere más que identificar al titular formal de la cuenta. Las credenciales pueden haber sido robadas, compartidas o utilizadas desde un dispositivo comprometido. Pooyandeh et al. (2022) señalan que los ataques contra identidades y sistemas pueden alterar registros y dificultar la identificación del responsable. La investigación debe considerar historiales de acceso, dispositivos, mecanismos de autenticación y patrones de actividad. Una dirección IP o un nombre de usuario constituyen indicios, pero no demuestran por sí solos la autoría.

La evidencia digital obtenida en el metaverso puede incorporarse a procesos ecuatorianos cuando sea posible demostrar su autenticidad, integridad y origen. Conversaciones, registros de acceso, movimientos, transacciones y archivos pueden representar hechos relevantes. El COGEP (2015) reconoce eficacia a los documentos digitales, pero su valoración exige información técnica suficiente. La naturaleza dinámica de las plataformas dificulta la conservación, pues los datos pueden modificarse o eliminarse rápidamente. Deben aplicarse medidas proporcionales que preserven lo necesario sin registrar de forma indiscriminada todas las actividades de los usuarios.

La cooperación del proveedor resulta especialmente importante cuando la evidencia permanece en servidores extranjeros. Las plataformas pueden conservar información sobre cuentas, comunicaciones, transacciones y dispositivos que no se encuentra disponible para la víctima. Sin embargo, la entrega de estos registros debe apoyarse en una solicitud legal y respetar los derechos de terceros. Chow et al. (2023) destacan que la arquitectura distribuida dificulta localizar datos y responsabilidades. La aplicación del derecho ecuatoriano requiere mecanismos de cooperación capaces de preservar evidencia sin extender la vigilancia más allá del incidente investigado.

La aplicación del derecho ecuatoriano también enfrenta límites prácticos. Una resolución puede resultar difícil de ejecutar cuando el proveedor carece de representación en el país, los activos se encuentran distribuidos o el responsable utiliza una identidad falsa. La tutela efectiva exige identificar al operador, localizar bienes o datos y lograr cooperación transfronteriza. Estas dificultades no eliminan la competencia ecuatoriana cuando existe conexión suficiente, pero demuestran que la eficacia jurídica depende tanto de las normas como de mecanismos técnicos, administrativos y judiciales de colaboración internacional.

1.7 Vacíos y desafíos normativos

El metaverso puede ser analizado mediante normas constitucionales, civiles, comerciales, penales y de protección de datos, pero el ordenamiento ecuatoriano todavía no contiene una regulación integral que identifique con precisión sus actores, riesgos y mecanismos de tutela. Esta ausencia no implica que los mundos virtuales carezcan de derecho aplicable. El problema surge cuando las categorías existentes resultan demasiado generales para responder a experiencias persistentes, inmersivas, automatizadas y transfronterizas. Kasiyanto y Kilinc (2022) sostienen que la regulación debe adaptarse a las funciones reales del entorno sin crear respuestas aisladas para cada innovación.

Uno de los principales desafíos consiste en definir qué debe entenderse jurídicamente por metaverso. Una definición excesivamente amplia podría incluir cualquier plataforma digital, mientras una formulación demasiado rígida quedaría rápidamente desactualizada. Song et al. (2023) muestran que estos entornos combinan inmersión, persistencia, interacción social y convergencia tecnológica con intensidades variables. La regulación debería centrarse en funciones y riesgos, como recopilación de datos, operaciones económicas, participación de menores o decisiones automatizadas, en lugar de depender únicamente de una categoría tecnológica cerrada.

La identificación de los responsables también presenta dificultades. En una misma experiencia pueden intervenir el operador de la plataforma, desarrolladores, fabricantes de dispositivos, proveedores de nube, comerciantes, moderadores y usuarios. La estructura descentralizada puede distribuir funciones sin eliminar el control real de determinados actores. Kasiyanto y Kilinc (2022) sostienen que la imputación debe atender a las funciones efectivamente ejercidas, la capacidad de control y la

intervención de cada participante. La regulación futura debe evitar tanto la inmunidad general de las plataformas como la atribución automática de toda conducta ejecutada por terceros.

Los datos generados por dispositivos inmersivos constituyen un desafío normativo específico. La LOPDP (2021) regula información personal, sensible y biométrica, pero la aplicación práctica puede resultar compleja frente a movimientos oculares, patrones corporales, reacciones fisiológicas y estimaciones emocionales. Sorrentino y López (2025) advierten que los entornos inmersivos producen datos observados e inferidos capaces de revelar características no comunicadas expresamente. Se requieren criterios técnicos que permitan determinar cuándo estas señales son biométricas, sensibles o de alto riesgo y qué medidas reforzadas deben aplicarse.

El consentimiento también necesita adaptación al diseño inmersivo. Las autorizaciones extensas y generales presentadas durante el registro no permiten comprender todos los tratamientos que pueden activarse posteriormente. Smith et al. (2025) señalan que la descentralización y la multiplicidad de actores dificultan identificar finalidades y destinatarios. La regulación debe exigir avisos contextuales, decisiones diferenciadas y mecanismos sencillos de revocación. Además, debe impedir que funciones esenciales se condicionen a tratamientos secundarios, como análisis emocional, publicidad conductual o reutilización de datos para finalidades no necesarias.

Las decisiones automatizadas representan otro campo insuficientemente desarrollado. Las plataformas pueden restringir cuentas, ordenar contenidos, modificar visibilidad, establecer recomendaciones o clasificar comportamientos mediante sistemas algorítmicos. La LOPDP (2021) reconoce garantías frente a valoraciones automatizadas, pero resulta necesario precisar cuándo una decisión produce una afectación significativa y qué explicación debe entregarse. La regulación debería exigir información comprensible, revisión humana real y mecanismos de impugnación. La supervisión no puede limitarse a confirmar automáticamente el resultado emitido por el mismo sistema cuestionado.

La evidencia digital requiere protocolos específicos de preservación. Los registros de acceso, movimientos de avatares, conversaciones y transacciones pueden permanecer bajo control exclusivo de empresas extranjeras y desaparecer rápidamente. Pooyandeh et al. (2022) señalan que los incidentes de seguridad pueden modificar registros y

dificultar la atribución. La regulación debe establecer procedimientos urgentes para conservar información, documentar su origen y garantizar integridad. Estas medidas deben limitarse al incidente investigado y evitar la grabación permanente e indiscriminada de todas las actividades realizadas por los participantes.

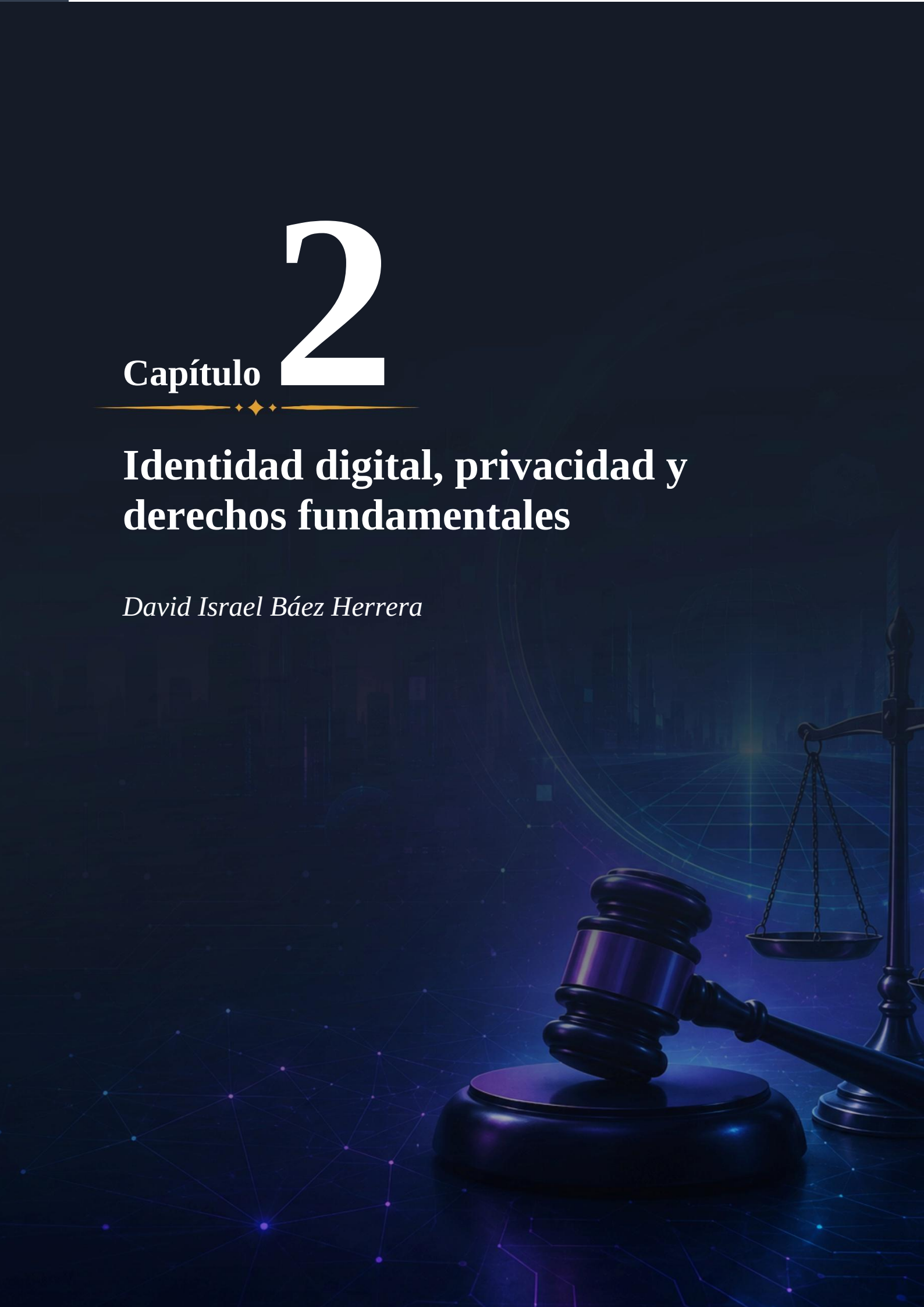
La respuesta regulatoria no debería consistir únicamente en crear nuevos delitos o una ley extensa para todas las plataformas. Un entorno educativo, un mercado de activos y una aplicación médica presentan riesgos distintos. La regulación basada en riesgos permitiría imponer obligaciones proporcionales según tratamiento de datos sensibles, participación de menores, valor económico, automatización y posibles daños físicos o psicológicos. Jauhiainen et al. (2023) sostienen que la sostenibilidad del metaverso depende de integrar dimensiones tecnológicas, sociales y regulatorias, evitando soluciones uniformes para contextos profundamente diferentes.

Los vacíos normativos del metaverso exigen, en consecuencia, una estrategia gradual y coordinada. Las normas vigentes ofrecen fundamentos importantes, pero deben complementarse con criterios técnicos, obligaciones de diseño y mecanismos de cooperación. La regulación futura debe identificar actores, distribuir responsabilidades y proteger derechos sin impedir la innovación. Un enfoque funcional y basado en riesgos permitirá adaptar el derecho ecuatoriano a nuevas plataformas sin crear categorías artificiales ni repetir disposiciones ya existentes. El objetivo debe ser asegurar tutela efectiva frente a consecuencias reales, independientemente del medio tecnológico utilizado.

Capítulo 2

Identidad digital, privacidad y derechos fundamentales

David Israel Báez Herrera



2.1 Identidad digital y avatares

La identidad digital comprende el conjunto de atributos, credenciales, comportamientos y representaciones que permiten individualizar a una persona dentro de un entorno tecnológico. En el metaverso, esta identidad no se limita al nombre de usuario o al correo registrado, sino que puede construirse mediante la apariencia del avatar, la voz, los movimientos, las relaciones, las adquisiciones y la reputación acumulada. Estos elementos forman una presencia virtual relativamente estable que puede proyectar consecuencias personales, sociales y patrimoniales fuera de la plataforma (Fernandez y Hui, 2022; Castillo et al., 2024).

El avatar constituye la manifestación visible y operativa de esa identidad dentro del mundo virtual. Puede adoptar una forma bidimensional, tridimensional, fantástica o hiperrealista y actuar como medio para comunicarse, desplazarse, crear contenidos y realizar operaciones. Su relevancia no depende únicamente de la semejanza física con el usuario, pues también puede adquirir reconocimiento mediante rasgos ficticios utilizados de manera constante. Castillo et al. (2024) explican que las herramientas de creación de avatares intervienen directamente en la construcción de la identidad y plantean desafíos de privacidad.

Jurídicamente, el avatar no posee personalidad autónoma ni compone un sujeto separado de quien lo controla. Carece de capacidad propia para adquirir derechos, asumir obligaciones o responder por daños. Las actuaciones ejecutadas mediante la representación deben atribuirse, según las circunstancias, a la persona natural o jurídica vinculada con la cuenta. No obstante, esa vinculación no puede presumirse de manera absoluta, porque las credenciales pueden haber sido compartidas, sustraídas o utilizadas desde un dispositivo comprometido. La atribución requiere examinar elementos técnicos y contextuales suficientes (Munn y Weijers, 2023).

La identidad digital tampoco debe confundirse con la identidad civil. Una persona puede utilizar un seudónimo, modificar su apariencia o asumir características distintas de las que posee en el espacio físico. Esta libertad permite explorar formas de expresión, participar sin revelar información innecesaria y reducir ciertos riesgos de discriminación. Munn y Weijers (2023) sostienen que los metaversos pueden ampliar posibilidades de autonomía y autorrepresentación, aunque sus estructuras también

pueden condicionar las opciones disponibles. La protección jurídica debe preservar esa libertad sin legitimar engaños, apropiaciones o daños contra terceros.

La Constitución de la República del Ecuador (2008), artículo 66, numeral 28, reconoce el derecho a la identidad personal y colectiva, incluyendo características materiales e inmateriales que individualizan a la persona. Esta garantía permite proteger representaciones virtuales cuando reproducen o se encuentran suficientemente vinculadas con alguien identificable. La tutela no convierte al avatar en una identidad jurídica distinta, sino que protege a la persona cuyos rasgos, voz, reputación o relaciones se proyectan mediante él. Su alcance debe determinarse considerando la posibilidad de reconocimiento y las consecuencias producidas por el uso cuestionado.

El libre desarrollo de la personalidad, reconocido en la Constitución de la República del Ecuador (2008), artículo 66, numeral 5, sustenta la posibilidad de configurar avatares conforme a preferencias individuales. Esta facultad comprende elegir apariencia, nombre, vestimenta y formas de interacción, siempre que no se afecten derechos ajenos. Las plataformas deberían evitar catálogos rígidos que excluyan identidades, culturas o capacidades diversas. Sin embargo, también deben impedir que la personalización sea utilizada para reproducir de manera engañosa a terceros, apropiarse de signos protegidos o construir representaciones destinadas a cometer fraude.

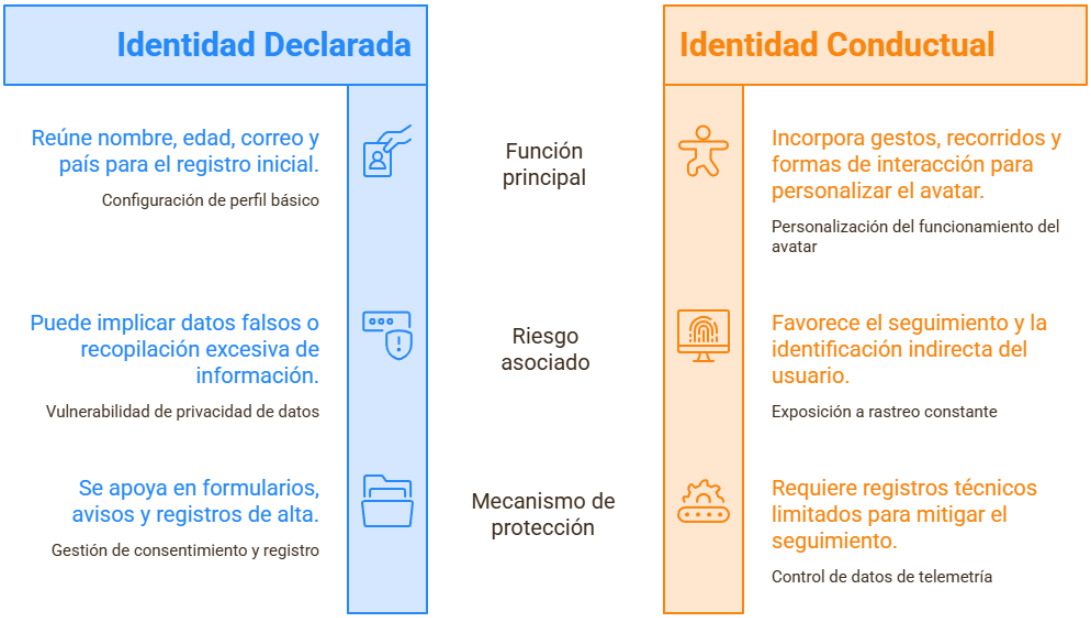
La utilización de seudónimos puede proteger la privacidad y favorecer la participación de personas expuestas a discriminación, represalias o vigilancia. El anonimato frente a otros usuarios no significa, sin embargo, que la actividad carezca de consecuencias jurídicas ni que el proveedor desconozca completamente al titular. Las plataformas suelen conservar direcciones electrónicas, dispositivos, registros de acceso y datos de pago capaces de relacionar la cuenta con una persona. Fernandez y Hui (2022) advierten que la acumulación de estos elementos permite reconstruir identidades incluso cuando el participante no revela públicamente su nombre civil.

La LOPDP (2021), artículo 4, considera dato personal cualquier información que identifica o hace identificable, directa o indirectamente, a una persona natural. El nombre del avatar, la apariencia, la voz, los contactos, las preferencias y el historial de actividad pueden quedar sometidos a protección cuando permiten individualizar al usuario. La calificación no depende de que cada elemento revele por sí solo la identidad. La combinación de señales aparentemente aisladas puede construir un perfil

suficientemente preciso para reconocer, seguir o clasificar a una persona dentro y fuera de la plataforma.

Los avatares hiperrealistas intensifican estos riesgos porque pueden construirse a partir de fotografías, grabaciones, escaneos y patrones corporales. Sorrentino y López (2025) señalan que la identidad virtual puede integrar datos biométricos e inferidos capaces de revelar características que el usuario no comunicó expresamente. La creación de una réplica detallada requiere definir qué información se utiliza, quién puede acceder a ella y si será reutilizada para publicidad, autenticación o entrenamiento algorítmico. La autorización para diseñar un avatar no comprende automáticamente cualquier finalidad posterior.

Figura 4
¿Qué capa de identidad digital priorizar para proteger en el metaverso?



Nota. La figura compara la identidad declarada y la identidad conductual según su función, los riesgos asociados y los mecanismos de protección aplicables en el metaverso. Elaboración propia.

La identidad representada por el avatar puede adquirir continuidad, reputación y valor económico a medida que el usuario participa en la plataforma. Una cuenta puede concentrar relaciones personales, antecedentes de moderación, creaciones propias, objetos adquiridos y oportunidades profesionales. La suspensión o eliminación de un avatar no siempre equivale a retirar una imagen decorativa. Puede afectar intereses acumulados durante largos periodos. Las decisiones de la plataforma deberían considerar la gravedad del incumplimiento, ofrecer información suficiente y permitir una revisión cuando la medida produzca consecuencias relevantes (Castillo et al., 2024).

La protección de la identidad también se relaciona con el honor, el buen nombre, la imagen y la voz. La Constitución de la República del Ecuador (2008), artículo 66, numeral 18, reconoce estos derechos y permite examinar la utilización de avatares creados para atribuir declaraciones, actos o comportamientos falsos. No toda semejanza constituye una vulneración, pues deben considerarse la finalidad artística, la parodia y la libertad de expresión. La afectación adquiere mayor intensidad cuando la representación busca engañar, desacreditar o aprovechar comercialmente el reconocimiento ajeno.

La suplantación puede producirse mediante el control ilegítimo de una cuenta o mediante la creación externa de una representación semejante. En el primer caso, el infractor utiliza credenciales ajenas; en el segundo, reproduce nombre, apariencia, voz o comportamiento para generar confusión. Esta diferencia resulta importante porque cada modalidad exige pruebas y respuestas distintas. Los mecanismos de autenticación permiten enfrentar la apropiación de cuentas, mientras las réplicas requieren procedimientos de identificación, retiro y rectificación. La inteligencia artificial aumenta la precisión de estas imitaciones y amplía sus posibles efectos (Fiaz et al., 2024).

Las plataformas deben incorporar medidas de protección proporcionales al valor personal y patrimonial de la identidad administrada. Entre ellas se encuentran la autenticación reforzada, las alertas de acceso, la recuperación segura, la verificación de cuentas institucionales y los canales rápidos para denunciar réplicas. Fiaz et al. (2024) proponen modelos de identidad autosoberana orientados a mejorar el control del usuario y reducir la exposición innecesaria de datos. Sin embargo, cualquier mecanismo debe evitar que la seguridad se convierta en una exigencia general de identificación biométrica o vigilancia permanente.

La identidad digital de niñas, niños y adolescentes requiere salvaguardas reforzadas. Sus avatares pueden revelar edad, institución educativa, preferencias, relaciones o ubicación aproximada, aun cuando no muestren el nombre real. La Constitución de la República del Ecuador (2008), artículos 44 y 45, exige priorizar su interés superior, identidad, integridad y dignidad. Las plataformas deberían configurar perfiles privados, limitar contactos con desconocidos y reducir la visibilidad de información. La protección no debe depender únicamente de la vigilancia familiar, porque el proveedor controla la arquitectura y las posibilidades de interacción.

La interoperabilidad plantea el desafío de trasladar la identidad entre diferentes entornos. Un usuario podría intentar conservar su avatar, reputación, credenciales o configuraciones al cambiar de plataforma. No obstante, la posibilidad técnica de transferir estos elementos no significa que todos deban viajar conjuntamente. La portabilidad debe diferenciar datos personales, componentes licenciados, relaciones con terceros y activos sujetos a reglas específicas. Sorrentino y López (2025) advierten que la circulación de información biométrica e inferida puede ampliar la vigilancia cuando distintos proveedores combinan los perfiles generados en cada entorno.

2.2 Datos personales y biométricos en el metaverso

El metaverso amplía considerablemente la cantidad y variedad de información generada por los usuarios. Además de nombres, correos electrónicos, credenciales y datos de pago, los entornos inmersivos pueden registrar voz, mirada, postura, movimientos corporales, expresiones faciales, ubicación y patrones de interacción. Esta información permite reproducir acciones, personalizar avatares y mejorar la experiencia, pero también facilita la identificación, vigilancia y elaboración de perfiles detallados. El tratamiento de datos en estos espacios requiere garantías superiores a las aplicadas en servicios digitales menos invasivos (Tukur et al., 2023).

La Constitución de la República del Ecuador (2008), artículo 66, numeral 19, reconoce el derecho a la protección de datos personales y la facultad de decidir sobre su recopilación, archivo, procesamiento, distribución y difusión. Esta garantía mantiene plena vigencia cuando la información es obtenida mediante visores, sensores, cámaras, micrófonos o dispositivos hápticos. La naturaleza virtual del entorno no disminuye la protección constitucional, porque los registros digitales pueden relacionarse con personas reales y utilizarse para influir en sus decisiones, oportunidades, reputación o acceso a determinados servicios.

La LOPDP (2021), artículo 4, considera dato personal toda información que identifica o hace identificable, directa o indirectamente, a una persona natural. No solo quedan protegidos los datos proporcionados durante el registro, sino también los historiales de actividad, identificadores técnicos, recorridos, contactos y preferencias vinculados con una cuenta. Incluso la apariencia o conducta de un avatar puede constituir información personal cuando permite reconocer al usuario o asociarlo razonablemente con otros registros disponibles para la plataforma, sus proveedores o terceros autorizados.

La identificación no siempre depende de un dato aislado. La combinación de dirección IP, dispositivo, voz, horarios, movimientos y relaciones puede reconstruir una identidad aunque el usuario participe mediante un seudónimo. Fernandez y Hui (2022) advierten que los entornos inmersivos permiten una observación más profunda que las plataformas tradicionales debido a la continuidad y riqueza de las señales recopiladas. La seudonimización reduce ciertos riesgos, pero no convierte automáticamente la información en anónima ni excluye la aplicación de la normativa de protección de datos.

Los datos biométricos presentan una sensibilidad particular porque derivan de características físicas, fisiológicas o conductuales estrechamente vinculadas con la persona. La LOPDP (2021), artículo 4, los define como información obtenida mediante un tratamiento técnico específico que permite o confirma una identificación única. Esta categoría puede comprender rostro, iris, huellas, voz, forma de caminar y patrones corporales. Sin embargo, un movimiento no se convierte automáticamente en dato biométrico: su calificación depende de que sea procesado técnicamente con una finalidad identificadora o de autenticación.

En el metaverso, una misma señal puede utilizarse para varios propósitos. El seguimiento ocular puede mejorar la representación visual, seleccionar objetos, medir la atención o inferir interés comercial. La voz puede facilitar una conversación, autenticar una cuenta o revelar emociones. Sorrentino y López (2025) destacan que los sistemas inmersivos pueden producir información biométrica e inferida que excede aquello que el usuario comunica conscientemente. Cada finalidad debe evaluarse de manera independiente y no presumirse autorizada por el simple uso del dispositivo.

Los datos inferidos representan uno de los mayores riesgos. A partir de movimientos, pausas, gestos, tono de voz o dirección de la mirada, los algoritmos pueden estimar emociones, preferencias, condiciones físicas, nivel de atención o probabilidad de compra. Estas conclusiones pueden ser inexactas y variar según cultura, discapacidad, edad o contexto. Aunque sean generadas por un sistema automatizado, continúan siendo datos personales cuando se vinculan con una persona identificable y pueden influir en decisiones comerciales, educativas, laborales o de moderación (Fernandez y Hui, 2022).

La siguiente tabla distingue las principales categorías de información tratadas en el metaverso y aporta criterios para determinar su nivel de riesgo y las medidas más

adecuadas. Su función no es repetir los principios legales, sino facilitar una clasificación operativa para evaluaciones de impacto y procesos de cumplimiento.

Tabla 4
Clasificación funcional de datos personales y biométricos en entornos inmersivos

Categoría	Ejemplos	Finalidad habitual	Nivel de riesgo	Medida prioritaria
Datos identificativos	Nombre, correo, edad y país	Registro y administración de la cuenta	Medio	Exactitud y control de acceso
Datos técnicos	IP, dispositivo, sistema y conexión	Seguridad y funcionamiento	Medio	Conservación limitada y seudonimización
Datos de comportamiento	Recorridos, compras, contactos y tiempo de uso	Personalización y análisis	Alto	Limitación de finalidad y oposición
Datos corporales	Postura, manos, cabeza y desplazamiento	Animación e interacción	Alto	Procesamiento local y minimización
Datos biométricos	Rostro, iris, voz o patrón de marcha	Identificación y autenticación	Muy alto	Cifrado, separación y acceso restringido
Datos fisiológicos	Ritmo cardíaco, reacción corporal y seguimiento ocular	Adaptación de la experiencia	Muy alto	Evaluación de impacto y tratamiento limitado
Datos inferidos	Emociones, atención, preferencias y nivel de riesgo	Perfilamiento y decisiones automatizadas	Muy alto	Transparencia, validación y revisión humana
Comunicaciones	Voz, mensajes y reuniones	Interacción entre participantes	Alto	Confidencialidad y prohibición de reutilización
Datos espaciales	Habitación, domicilio aproximado y entorno físico	Seguridad y realidad aumentada	Muy alto	Precisión reducida y procesamiento en el dispositivo
Datos de menores	Voz, edad, contactos, hábitos y ubicación	Acceso y personalización	Muy alto	Privacidad por defecto y prohibición de usos comerciales invasivos

Nota. El nivel de riesgo aumenta cuando la información permite identificación permanente, genera inferencias sensibles o se utiliza para adoptar decisiones que afectan al usuario.

La LOPDP (2021), artículo 7, exige que todo tratamiento disponga de una base legitimadora. La plataforma debe identificar por separado el fundamento jurídico de

cada operación, evitando presentar una aceptación general como autorización para cualquier finalidad. Los datos estrictamente necesarios para prestar el servicio pueden responder a la ejecución contractual, mientras la publicidad conductual, el análisis emocional o el entrenamiento de sistemas pueden requerir otra base. Esta diferenciación impide que funciones secundarias se oculten bajo la apariencia de requisitos técnicos indispensables.

Cuando se utilice el consentimiento, este debe cumplir las condiciones establecidas en la LOPDP (2021), artículo 8. La autorización debe ser libre, específica, informada e inequívoca, y no puede derivarse de la mera permanencia en el entorno. En una plataforma inmersiva, los avisos deben aparecer en el momento en que se active una cámara, micrófono, sensor corporal o herramienta de análisis. La persona debe poder rechazar los tratamientos opcionales sin perder injustificadamente el acceso a las funciones principales del servicio.

Los principios del artículo 10 de la LOPDP (2021) deben aplicarse mediante decisiones técnicas verificables. La minimización exige captar únicamente la información indispensable; la finalidad impide reutilizarla para objetivos incompatibles; la proporcionalidad obliga a valorar alternativas menos invasivas; y la conservación limitada requiere eliminarla cuando deje de ser necesaria. Tukur et al. (2023) señalan que la recopilación permanente aumenta la exposición frente a accesos ilícitos, filtraciones y usos secundarios. Resulta preferible procesar determinadas señales dentro del dispositivo sin transmitirlas al servidor.

La seguridad debe considerar que los datos biométricos no pueden sustituirse fácilmente. Una contraseña comprometida puede modificarse, pero el rostro, el iris o la voz permanecen asociados con la persona. La LOPDP (2021), artículo 38, exige políticas, análisis de riesgos y medidas técnicas y organizativas apropiadas. Fiaz et al. (2024) destacan la utilidad de arquitecturas de identidad y protección descentralizada, aunque estas soluciones no eliminan los riesgos. Las plantillas biométricas deben cifrarse, separarse de otros registros y limitarse a los actores estrictamente autorizados.

La protección de datos desde el diseño exige incorporar controles antes de implementar la plataforma. Las configuraciones iniciales deberían reducir la visibilidad del perfil, desactivar grabaciones innecesarias y restringir el acceso de aplicaciones externas a sensores corporales. Castillo et al. (2024) señalan que las herramientas de creación de

avatares pueden recopilar información personal durante la personalización, por lo que sus interfaces deben explicar qué elementos se almacenan. La protección por defecto resulta especialmente importante cuando el usuario desconoce la capacidad técnica de los dispositivos utilizados.

Las comunicaciones y transferencias internacionales añaden complejidad porque una misma experiencia puede involucrar al operador, fabricantes, proveedores de almacenamiento, anunciantes y desarrolladores ubicados en distintos países. El usuario debe conocer quién determina las finalidades, qué entidades reciben los datos y dónde se procesan. La contratación de terceros no elimina la responsabilidad del operador. Smith et al. (2025) advierten que la arquitectura distribuida amplía la superficie de exposición y dificulta identificar al actor responsable cuando se produce una vulneración.

Los derechos de acceso, rectificación, eliminación y oposición permiten que la persona controle los datos generados durante la experiencia. Su ejercicio debe comprender no solo la información proporcionada, sino también los perfiles, registros conductuales e inferencias asociadas. Una respuesta basada exclusivamente en datos visibles de la cuenta sería insuficiente. La plataforma debe explicar el significado de los registros técnicos y corregir las consecuencias producidas por datos inexactos. Esta cuestión se desarrollará con mayor amplitud en el apartado dedicado al hábeas data y la tutela digital.

La protección debe intensificarse cuando los datos corresponden a niñas, niños o adolescentes. Las plataformas pueden recopilar desde edades tempranas información sobre voz, movimientos, relaciones, emociones y preferencias, construyendo perfiles de larga duración. La Constitución de la República del Ecuador (2008), artículos 44 y 45, exige priorizar su interés superior e integridad. Las cuentas de menores deben utilizar privacidad por defecto, recopilación mínima y límites estrictos al perfilamiento, evitando que la autorización familiar sea utilizada para justificar tratamientos innecesarios o comercialmente invasivos.

Los datos personales y biométricos constituyen uno de los principales ámbitos de riesgo jurídico del metaverso. Su protección exige reconocer que la información corporal, conductual e inferida puede revelar más de lo que el usuario decide comunicar. La normativa ecuatoriana proporciona bases suficientes sobre legitimidad, finalidad,

seguridad y control, pero su aplicación debe traducirse en medidas técnicas concretas. La innovación inmersiva será compatible con los derechos cuando reduzca la recopilación, limite las inferencias y preserve el control de la persona sobre su identidad y comportamiento digital (Sorrentino y López, 2025).

2.3 Consentimiento y autodeterminación informativa

La autodeterminación informativa reconoce la facultad de cada persona para conocer, decidir y controlar el tratamiento de sus datos personales. En el metaverso, esta potestad adquiere especial importancia porque la información puede recopilarse de manera continua mediante sensores, cámaras, micrófonos y dispositivos hápticos. El usuario no solo debe decidir qué datos entrega directamente, sino también comprender qué señales se observan, qué inferencias se generan y cómo pueden utilizarse posteriormente. La intensidad de esta vigilancia exige mecanismos de control adaptados a la experiencia inmersiva (Fernandez y Hui, 2022).

La Constitución de la República del Ecuador (2008), artículo 66, numeral 19, reconoce el derecho a la protección de datos personales, incluyendo el acceso y la decisión sobre la información relacionada con una persona. Esta garantía constituye el fundamento constitucional de la autodeterminación informativa. Su aplicación impide considerar que el ingreso a una plataforma equivale a una renuncia general sobre la voz, los movimientos, la mirada, las conversaciones o los perfiles generados. La persona conserva facultades de decisión incluso cuando los datos son captados automáticamente durante la interacción virtual.

El consentimiento establece una de las bases legitimadoras previstas en la LOPDP (2021), artículo 7, pero no debe emplearse de manera indiscriminada. Algunas operaciones pueden ser necesarias para ejecutar un contrato, cumplir una obligación legal o proteger intereses legítimos bajo condiciones específicas. Solicitar autorización para todo tratamiento puede producir una apariencia falsa de libertad cuando el usuario no dispone realmente de alternativas. El responsable debe identificar el fundamento jurídico correspondiente a cada finalidad y explicar por qué determinada información resulta necesaria para la función ofrecida.

Cuando el tratamiento se sustenta en el consentimiento, la LOPDP (2021), artículo 8, exige que este sea libre, específico, informado e inequívoco. Estas condiciones deben cumplirse de forma conjunta y no únicamente mediante la aceptación formal de una

política de privacidad. Smith et al. (2025) advierten que los entornos descentralizados dificultan identificar responsables, finalidades y destinatarios, lo que puede debilitar la calidad de la autorización. La complejidad tecnológica no elimina la obligación de presentar opciones comprensibles y demostrar que la decisión fue voluntaria.

La libertad del consentimiento requiere que el usuario pueda rechazar tratamientos opcionales sin sufrir consecuencias desproporcionadas. No existe una elección real cuando la plataforma condiciona funciones esenciales a la aceptación de publicidad conductual, seguimiento emocional o transferencia de datos a múltiples terceros. Esta dificultad aumenta en espacios educativos o laborales, donde la participación puede ser obligatoria. En tales situaciones, el consentimiento puede no constituir una base adecuada, por lo que deben evaluarse otros fundamentos jurídicos y reducirse la recopilación a lo estrictamente indispensable (Smith et al., 2025).

La especificidad impide reunir finalidades distintas bajo una autorización única. Permitir la creación de una cuenta o la animación de un avatar no comprende, por ese solo hecho, el reconocimiento facial, el análisis emocional, la personalización publicitaria ni el entrenamiento de sistemas de inteligencia artificial. Cada propósito requiere una decisión diferenciada cuando pueda aceptarse o rechazarse de manera independiente. Esta separación permite retirar una autorización secundaria sin perder injustificadamente las funciones principales del servicio y evita que la acumulación de propósitos reduzca el control efectivo de la persona sobre su información (Smith et al., 2025).

La información constituye una condición material de validez y no una formalidad satisfecha mediante políticas extensas. El usuario necesita conocer previamente qué datos serán recopilados, con qué finalidad, durante cuánto tiempo y qué entidades podrán recibirlos. El artículo 12 de la LOPDP (2021) exige una comunicación clara sobre el tratamiento, mientras la multiplicidad de actores descrita por Smith et al. (2025) refuerza la necesidad de avisos escalonados. En una experiencia inmersiva, la advertencia debe aparecer cuando se activa una grabación, comienza el seguimiento ocular o una aplicación externa obtiene acceso a señales corporales.

La manifestación inequívoca exige una acción afirmativa que permita comprobar la voluntad del usuario. El silencio, la inactividad, las casillas previamente seleccionadas o la simple permanencia en un espacio virtual no deberían interpretarse como

aceptación. Tampoco un gesto cotidiano puede adquirir consecuencias jurídicas si la persona desconoce su significado dentro de la interfaz. Los comandos de voz, movimientos o selecciones virtuales pueden expresar consentimiento, pero deben estar acompañados por información clara, confirmación suficiente y posibilidad de cancelar la decisión antes de que comience el tratamiento.

El diseño de la interfaz puede fortalecer o debilitar la autonomía informativa. Colores, tamaños, recorridos, sonidos y recompensas pueden dirigir al usuario hacia la opción más favorable para la plataforma. Una aceptación destacada frente a un rechazo oculto constituye una práctica manipulativa incompatible con la lealtad y transparencia previstas en la LOPDP (2021), artículo 10. Las opciones deben presentarse con similar visibilidad y lenguaje neutral. La experiencia inmersiva no debe utilizarse para convertir decisiones jurídicas en acciones apresuradas o emocionalmente condicionadas.

Sakka et al. (2026) sostienen que los límites digitales deben poder expresarse y modificarse durante la experiencia, no únicamente al ingresar a la plataforma. Este enfoque resulta especialmente relevante en interacciones corporales, hápticas o espaciales. El usuario debe poder aceptar una actividad, restringir determinados contactos y retirar posteriormente su autorización. El consentimiento inicial no representa una autorización permanente ni general para cualquier estímulo. Las zonas personales, bloqueos y controles de proximidad permiten materializar la autonomía mediante decisiones inmediatas integradas en la arquitectura tecnológica.

La revocación compone una dimensión esencial de la autodeterminación informativa. La LOPDP (2021), artículo 8, permite retirar el consentimiento en cualquier momento sin afectar la licitud del tratamiento realizado previamente. El retiro debe ser tan sencillo como la aceptación y no requerir formularios complejos, comunicaciones físicas o cierre definitivo de la cuenta. La plataforma debe explicar qué funciones se verán realmente afectadas y evitar consecuencias diseñadas únicamente para desincentivar la revocación. Los tratamientos secundarios deben cesar cuando pierdan su fundamento jurídico.

Retirar el consentimiento no implica siempre la eliminación inmediata de toda la información. Algunos datos pueden conservarse cuando exista una obligación legal, otra base legitimadora o necesidad de formular y defender reclamaciones. Sin embargo,

el responsable debe restringir su utilización y explicar claramente el motivo de la conservación. Los registros biométricos recopilados para personalizar un avatar no deberían continuar utilizándose con fines publicitarios después de la revocación. La permanencia técnica de los datos no autoriza mantener todas las operaciones previamente asociadas con ellos.

La autodeterminación informativa también se ejerce mediante los derechos de acceso, rectificación, eliminación y oposición. Estas facultades permiten conocer los datos tratados, corregir registros inexactos y detener usos que carezcan de justificación suficiente. En el metaverso, su ejercicio debe comprender la información proporcionada, los comportamientos observados y las inferencias generadas. La persona debe conocer no solo qué datos existen, sino cómo influyen en recomendaciones, restricciones o decisiones. Su desarrollo jurisdiccional será abordado específicamente en el apartado sobre hábeas data y tutela digital.

La Sentencia 001-14-PJO-CC (2014) de la Corte Constitucional del Ecuador aporta criterios relevantes sobre el control que corresponde a la persona respecto de su información. Esta jurisprudencia permite reforzar la idea de que el consentimiento no agota la protección de los datos personales ni elimina las facultades posteriores del titular. La autorización debe interpretarse dentro de un sistema de derechos que incluye acceso, conocimiento, rectificación y control sobre la utilización. En entornos inmersivos, esta perspectiva impide transformar una aceptación inicial en un permiso ilimitado e irreversible.

La Sentencia 59-19-IN/24 (2024) también puede sustentar una interpretación reforzada frente a tratamientos capaces de afectar derechos fundamentales. Su incorporación resulta pertinente cuando la recopilación es intensa, involucra categorías sensibles o se aplica a personas en situación de vulnerabilidad. La existencia formal del consentimiento no elimina la obligación de examinar necesidad, proporcionalidad y finalidad. Una plataforma no puede justificar el seguimiento emocional permanente o la observación biométrica excesiva únicamente porque el usuario marcó una casilla durante el registro.

Las niñas, niños y adolescentes requieren explicaciones adecuadas a su edad y nivel de comprensión. La intervención de sus representantes no convierte en legítimo cualquier tratamiento ni sustituye por completo la opinión del menor. Las plataformas deben

aplicar privacidad por defecto, limitar finalidades comerciales y ofrecer controles comprensibles. La autonomía progresiva exige reconocer una participación creciente en decisiones sobre identidad, contactos y datos personales. La autorización familiar debe orientarse al interés superior y no utilizarse como una renuncia general a la intimidad o protección informativa.

2.4 Intimidad, imagen y libertad de expresión

La participación en el metaverso modifica las condiciones en las que se ejercen la intimidad, la propia imagen y la libertad de expresión. Las personas pueden conversar, asistir a reuniones, crear contenidos y representar identidades mediante avatares, pero estas actividades pueden ser observadas y registradas de manera continua. La voz, los gestos, los movimientos y los espacios físicos captados por dispositivos inmersivos permiten reconstruir aspectos de la vida personal. La protección jurídica debe considerar tanto el contenido comunicado como la arquitectura tecnológica que posibilita su seguimiento (Fernandez y Hui, 2022).

La intimidad protege un ámbito reservado de la vida personal y familiar frente a accesos, observaciones o divulgaciones injustificadas. La Constitución de la República del Ecuador (2008), artículo 66, numeral 20, reconoce expresamente este derecho. Su aplicación no depende de que la persona se encuentre en un espacio físico privado. Una sala virtual restringida, una consulta profesional o una reunión familiar pueden generar una expectativa legítima de reserva, aunque la comunicación sea procesada por servidores administrados por una empresa privada o se realice mediante avatares.

La expectativa de intimidad varía según las características del espacio virtual. Un evento abierto al público no ofrece el mismo grado de reserva que una sala protegida mediante invitación o contraseña. Sin embargo, participar en un entorno público no implica aceptar cualquier forma de seguimiento, grabación o perfilamiento. La plataforma debe diferenciar entre la información necesaria para mostrar la interacción y aquella que pretende conservar o reutilizar. Fernandez y Hui (2022) advierten que la arquitectura del metaverso puede convertir actividades aparentemente ordinarias en fuentes permanentes de observación.

La intimidad también puede afectarse mediante inferencias. El usuario quizá no revele directamente sus emociones, preferencias, salud o relaciones, pero los sistemas pueden intentar deducirlas a partir de su voz, mirada, distancia corporal y comportamiento.

Sorrentino y López (2025) destacan que los avatares y dispositivos inmersivos generan datos biométricos e inferidos capaces de revelar características no expresadas conscientemente. La protección no debe limitarse a la información declarada, pues una conclusión algorítmica puede resultar igualmente invasiva y producir decisiones desfavorables.

La inviolabilidad de las comunicaciones constituye una dimensión específica de la intimidad. La Constitución de la República del Ecuador (2008), artículo 66, numeral 21, protege el secreto de la correspondencia física y virtual. Esta garantía comprende mensajes privados, conversaciones de voz y comunicaciones mantenidas en espacios restringidos. Las plataformas deben impedir accesos injustificados por parte de usuarios, administradores o aplicaciones externas. La conservación técnica de una comunicación no autoriza su lectura, grabación o reutilización para publicidad, entrenamiento algorítmico o vigilancia sin una base jurídica suficiente.

La imagen y la voz constituyen manifestaciones de la personalidad capaces de identificar a una persona. La Constitución de la República del Ecuador (2008), artículo 66, numeral 18, protege el honor, el buen nombre, la imagen y la voz. En el metaverso, esta tutela comprende fotografías, grabaciones, escaneos tridimensionales y avatares que reproduzcan características reconocibles. Castillo et al. (2024) señalan que las herramientas de creación de avatares intervienen en la construcción de la identidad y pueden generar riesgos cuando utilizan o conservan rasgos personales sin controles suficientes.

La protección de la imagen no exige necesariamente una reproducción exacta del rostro. Una combinación de voz, vestimenta, cuerpo, movimientos, nombre y contexto puede permitir que terceros identifiquen a la persona representada. La relevancia jurídica depende del grado de reconocimiento, la autorización otorgada, la finalidad del uso y los efectos ocasionados. Una representación ficticia claramente diferenciada no recibe el mismo tratamiento que una réplica diseñada para aparentar que alguien participó en una conducta, realizó una declaración o autorizó una operación que nunca ocurrió.

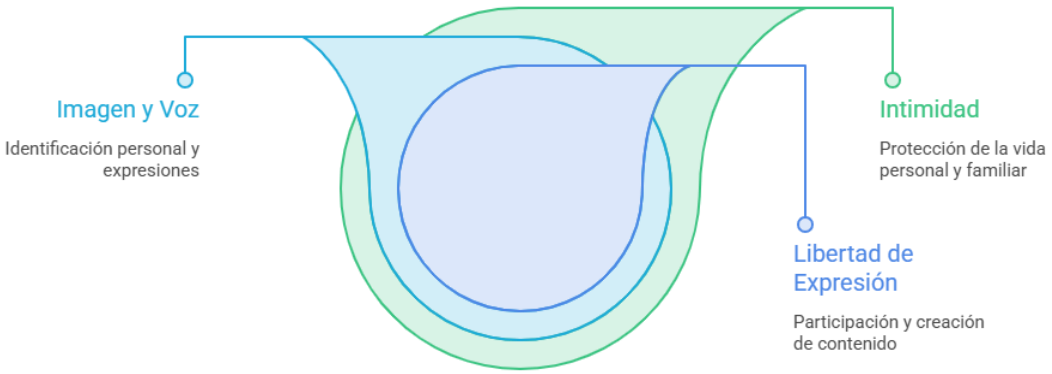
Las réplicas digitales generadas mediante inteligencia artificial intensifican estos riesgos. Una plataforma o usuario puede reproducir rostro, voz, gestos y movimientos con suficiente precisión para inducir a error. Estas representaciones pueden emplearse en publicidad, fraude, escenas íntimas o mensajes falsos. Sorrentino y López (2025)

advierten que la combinación de información biométrica e inferida incrementa las posibilidades de reproducción y manipulación de identidades. Las plataformas deben permitir identificar contenidos sintéticos, denunciar réplicas no autorizadas y retirar oportunamente aquellas que ocasionen daños.

La protección de la imagen no concede un derecho absoluto para impedir cualquier representación. Debe armonizarse con la libertad de expresión, el derecho a informar, la crítica, la creación artística y la parodia. Una caricatura claramente identificada puede contribuir al debate público, mientras una réplica hiperrealista presentada como auténtica puede generar engaño y daño reputacional. La ponderación debe considerar si la representación posee interés público, si se advierte su carácter ficticio y si revela aspectos pertenecientes a la vida íntima de la persona afectada.

La Sentencia 2064-14-EP/21 (2021) de la Corte Constitucional del Ecuador aporta criterios pertinentes para analizar la relación entre privacidad, imagen y circulación de información. Su incorporación permite reforzar que la divulgación de datos o contenidos personales debe examinarse según el contexto, la finalidad y la afectación ocasionada. En el metaverso, la mera accesibilidad técnica de una imagen o conversación no significa que pueda difundirse sin límites. La protección constitucional subsiste cuando la reutilización altera el contexto original o amplía injustificadamente la exposición del titular.

Figura 5
Protección de la intimidad, imagen y libertad de expresión en el metaverso



Nota. La figura muestra la relación entre la intimidad, la imagen y voz, y la libertad de expresión en el metaverso. Elaboración propia.

La libertad de expresión está reconocida en la Constitución de la República del Ecuador (2008), artículo 66, numeral 6, y permite opinar y expresar el pensamiento en todas sus formas. El metaverso amplía estas posibilidades mediante voz, texto, gestos, diseños, actuaciones y configuraciones de avatares. La libertad comprende expresiones

favorables, críticas o incómodas, por lo que las plataformas no deberían retirar contenidos únicamente por resultar impopulares. Sin embargo, su ejercicio debe respetar los derechos a la dignidad, igualdad, intimidad, honor y seguridad de los demás participantes.

La Constitución de la República del Ecuador (2008), artículo 16, reconoce además una comunicación libre, intercultural, incluyente, diversa y participativa. Esta garantía adquiere relevancia porque las plataformas controlan la visibilidad, circulación y permanencia de las expresiones. Los algoritmos pueden priorizar determinados discursos, reducir el alcance de otros o excluir usuarios de espacios relevantes. La arquitectura tecnológica funciona, por tanto, como una forma de regulación material. La transparencia sobre recomendaciones y restricciones resulta indispensable para evitar que decisiones comerciales ocultas condicionen injustificadamente la participación.

El anonimato y el seudonimato pueden favorecer la libertad de expresión de personas expuestas a discriminación, represalias o vigilancia. Obligar a mostrar públicamente la identidad civil puede excluir a víctimas, denunciantes o integrantes de grupos vulnerables. Sin embargo, la protección del anonimato no significa que las conductas ilícitas queden impunes. La identificación del responsable debe realizarse mediante procedimientos legales y proporcionales. Munn y Weijers (2023) sostienen que la autonomía virtual requiere preservar formas legítimas de representación sin eliminar la responsabilidad frente a daños verificables.

La moderación constituye una función necesaria para prevenir amenazas, acoso, discriminación y difusión de contenidos íntimos. No obstante, puede convertirse en censura privada cuando sus reglas son ambiguas o se aplican sin contexto. Chawki et al. (2024) destaca que los daños producidos en entornos virtuales requieren respuestas capaces de reconocer la intensidad de la experiencia sin equiparar automáticamente toda conducta con una agresión física. Las plataformas deben distinguir entre conflicto, ficción, crítica legítima y comportamiento destinado a intimidar o vulnerar derechos.

Los sistemas automatizados de moderación presentan dificultades para interpretar ironía, idioma, discapacidad, expresiones culturales y consentimiento. Una palabra o gesto puede tener significados distintos según el contexto. La LOPDP (2021), artículo 20, resulta pertinente cuando la reducción de visibilidad, suspensión o eliminación

deriva de valoraciones automatizadas que afectan significativamente derechos y libertades. El usuario debe conocer la regla aplicada, recibir una explicación comprensible y solicitar revisión humana. La mera afirmación de que el algoritmo detectó una infracción no constituye una respuesta suficiente.

Las medidas de moderación deben ser proporcionales a la gravedad y reiteración de la conducta. Una infracción leve puede justificar una advertencia o restricción temporal, mientras amenazas, persecución o difusión de contenido íntimo pueden exigir bloqueo inmediato y preservación de evidencia. La cancelación definitiva de una cuenta requiere especial cautela cuando contiene relaciones, obras, actividades profesionales o activos adquiridos. La protección de la víctima no exige eliminar toda posibilidad de defensa, pero la revisión tampoco debe prolongar innecesariamente la exposición al daño (Chawki et al., 2024).

La difusión no consentida de conversaciones, imágenes o escenas íntimas puede causar una afectación continuada debido a la facilidad para copiar y trasladar contenidos entre plataformas. La respuesta debe ser rápida y evitar que la conservación probatoria sirva como argumento para mantener públicamente el material. El operador puede retirar el contenido y conservar una copia restringida durante el tiempo necesario para investigar. La eliminación visible, la rectificación y la reparación deben coordinarse con la protección de la evidencia y la confidencialidad de la persona afectada.

2.5 Protección de menores en el metaverso

La participación de niñas, niños y adolescentes en el metaverso puede favorecer experiencias educativas, recreativas y sociales, pero también intensifica riesgos vinculados con privacidad, contacto con desconocidos, publicidad, compras y violencia virtual. La sensación de presencia generada por los entornos inmersivos puede hacer que las interacciones resulten emocionalmente más significativas que en otros medios digitales. La protección no debe limitarse a reaccionar después de una vulneración, sino incorporarse desde el diseño, la configuración y la administración de las plataformas (Munn y Weijers, 2023).

La Constitución de la República del Ecuador (2008), artículo 44, establece que el Estado, la sociedad y la familia deben promover prioritariamente el desarrollo integral de niñas, niños y adolescentes. Además, determina que su interés superior prevalecerá sobre los derechos de las demás personas. Este principio exige que las decisiones

tecnológicas, contractuales y comerciales adoptadas por las plataformas consideren principalmente la seguridad, dignidad y bienestar del menor, incluso cuando entren en conflicto con objetivos como incrementar el tiempo de conexión, recopilar más información o maximizar ingresos publicitarios.

La protección constitucional comprende también la integridad, identidad, educación, participación y dignidad. La Constitución de la República del Ecuador (2008), artículo 45, reconoce que niñas, niños y adolescentes son titulares de los derechos comunes del ser humano y de aquellos específicos de su edad. Las agresiones realizadas mediante avatares, la difusión de imágenes, la apropiación de identidades o la exposición a contenidos perjudiciales pueden afectar derechos reales. La virtualidad del medio no reduce la obligación de prevenir, investigar y reparar las consecuencias ocasionadas.

El Código de la Niñez y Adolescencia (2003), artículo 11, reconoce el interés superior como principio orientado a garantizar el ejercicio efectivo de los derechos de los menores. Su aplicación en el metaverso requiere examinar la edad, madurez, finalidad de la plataforma, intensidad de la inmersión y posibilidad de interacción con adultos. No todas las experiencias presentan el mismo nivel de riesgo. Un entorno educativo supervisado exige medidas distintas de una plataforma abierta con mensajería privada, economía interna y espacios administrados por los propios usuarios.

La autonomía progresiva impide considerar a los menores únicamente como sujetos pasivos de protección. Conforme desarrollan su capacidad de comprensión, deben participar en las decisiones relacionadas con privacidad, identidad, contactos y publicación de contenidos. Las explicaciones deben adaptarse a su edad y permitirles identificar riesgos, modificar configuraciones y solicitar ayuda. La intervención de los representantes legales continúa siendo necesaria, pero no debe transformarse en vigilancia ilimitada. Proteger al menor también implica respetar gradualmente su intimidad, opinión y capacidad de participación.

La verificación de edad constituye uno de los desafíos más complejos. Una simple declaración puede ser fácilmente eludida, mientras la exigencia de documentos, reconocimiento facial o estimaciones biométricas puede aumentar la recopilación de datos sensibles. El mecanismo debe guardar relación con el riesgo del servicio y limitarse a confirmar un rango etario cuando no sea indispensable conocer la identidad civil. Sorrentino y López (2025) advierten que la recopilación intensiva amplía las

posibilidades de seguimiento, filtración y reutilización incompatible de información personal.

Los sistemas automatizados de estimación de edad también pueden cometer errores. La apariencia, la voz y el comportamiento no permiten determinar con absoluta precisión la edad de una persona y pueden variar por factores culturales, físicos o médicos. Una clasificación equivocada podría permitir que un niño acceda a contenidos inadecuados o impedir que un adolescente utilice legítimamente un servicio. Cuando estas decisiones afecten significativamente su acceso, deben existir explicaciones comprensibles, mecanismos de corrección y revisión humana conforme a las garantías de la LOPDP (2021), artículo 20.

La privacidad por defecto debe constituir la configuración inicial de las cuentas pertenecientes a menores. Los perfiles no deberían mostrar públicamente su nombre, ubicación, institución educativa, lista de contactos o historial de actividad. La LOPDP (2021), artículo 10, exige aplicar los principios de finalidad, minimización, proporcionalidad, confidencialidad y seguridad. Por tanto, las funciones de mayor exposición deben permanecer desactivadas hasta que exista una decisión apropiada para la edad y suficientemente informada, sin emplear diseños que presionen al usuario para ampliar su visibilidad.

Tabla 5
Matriz de protección integral de menores en el metaverso

Área de riesgo	**Situación que debe prevenirse**	**Medida incorporada por defecto**	**Intervención posterior requerida**	**Actor principalmente responsable**
Identidad	Exposición del nombre, edad o institución educativa	Perfil privado y seudónimo	Retiro de información divulgada	Plataforma y representantes
Contacto	Mensajes o invitaciones de adultos desconocidos	Restricción de comunicaciones privadas	Bloqueo, investigación y seguimiento	Plataforma
Datos corporales	Captura continua de voz, mirada o movimientos	Procesamiento local y recopilación mínima	Eliminación o restricción del registro	Responsable del tratamiento

Área de riesgo	Situación que debe prevenirse	Medida incorporada por defecto	Intervención posterior requerida	Actor principalmente responsable
Contenido	Acceso a violencia, sexualización o discriminación	Clasificación etaria y filtros graduados	Revisión contextual del contenido	Plataforma y moderadores
Ciberacoso	Persecución, insultos o gestos invasivos	Espacio personal, bloqueo y salida rápida	Preservación de evidencia y apoyo	Plataforma e institución vinculada
Publicidad	Promociones encubiertas o perfilamiento emocional	Desactivación de publicidad conductual	Retiro de campañas manipulativas	Plataforma y anunciante
Compras	Adquisiciones impulsivas o no autorizadas	Límites de gasto y confirmación adicional	Reembolso y revisión de la operación	Proveedor y representante
Suplantación	Copia del avatar, voz o nombre del menor	Autenticación segura y controles de réplica	Retiro, rectificación y denuncia	Plataforma
Uso excesivo	Recompensas y estímulos que prolongan la conexión	Pausas, recordatorios y límites configurables	Evaluación de patrones perjudiciales	Plataforma y familia
Seguridad física	Caídas, fatiga o desorientación	Advertencias, límites espaciales y pausas	Atención del incidente y revisión técnica	Fabricante y plataforma

Nota. La matriz diferencia las medidas que deben existir antes del riesgo de aquellas que se activan cuando el incidente ya se ha producido.

La protección frente al contacto con desconocidos constituye una obligación prioritaria. La comunicación por voz, los gestos y la proximidad entre avatares pueden generar una sensación de confianza y cercanía. Las cuentas de menores deberían restringir por defecto mensajes privados, invitaciones a espacios aislados y comunicaciones con adultos no verificados. Jauhiainen et al. (2023) señalan que la dimensión social de los mundos virtuales puede ampliar oportunidades de participación, pero también reproducir exclusión, manipulación y relaciones desiguales entre participantes.

La captación y manipulación pueden desarrollarse mediante acercamientos progresivos, ofrecimiento de regalos virtuales, generación de confianza y solicitud de información privada. El uso de avatares ficticios dificulta conocer la edad o identidad real del interlocutor. Las plataformas deben analizar patrones de riesgo sin convertir todas las

comunicaciones en objeto de vigilancia indiscriminada. La prevención debe apoyarse en restricciones de contacto, alertas comprensibles, moderación especializada y canales de denuncia capaces de intervenir cuando existan indicios concretos de peligro.

El ciberacoso inmersivo puede manifestarse mediante insultos, persecución del avatar, exclusión de actividades, invasión del espacio personal o gestos sexualizados. La presencia virtual puede intensificar la percepción de amenaza y ocasionar miedo, ansiedad o abandono del entorno. Chawki et al. (2024) sostiene que los daños virtuales requieren respuestas jurídicas y tecnológicas coordinadas, especialmente cuando las conductas afectan la integridad y dignidad. Las plataformas deben ofrecer bloqueo inmediato, zonas personales, silenciamiento y mecanismos que permitan abandonar una interacción sin perder completamente el acceso al servicio.

Las herramientas de denuncia deben ser visibles, sencillas y adecuadas para la edad. Un menor no debería completar formularios complejos ni describir jurídicamente la conducta para recibir ayuda. El sistema puede permitir bloquear al usuario, preservar temporalmente registros y comunicar el incidente a un moderador capacitado. La denuncia debe generar una confirmación y evitar que la persona afectada repita innecesariamente la experiencia. También debe protegerse su identidad durante la investigación y limitarse el acceso a la información estrictamente necesaria.

La publicidad inmersiva representa un riesgo cuando se integra de forma poco visible en objetos, personajes, recompensas o experiencias sociales. Los menores pueden tener dificultades para distinguir entre contenido recreativo, recomendación y promoción comercial. El análisis de emociones, preferencias y vulnerabilidades permite personalizar mensajes con una intensidad superior a la publicidad convencional. La protección debe impedir el perfilamiento comercial invasivo y exigir que toda promoción sea claramente identificable, evitando estímulos que exploten la inexperiencia o la presión del grupo.

Las economías internas también pueden ocultar el costo real de las decisiones. Las monedas virtuales, objetos de edición limitada y recompensas aleatorias pueden dificultar que el menor comprenda cuánto dinero está utilizando. La Ley Orgánica de Defensa del Consumidor (2000) exige información clara y protege frente a prácticas engañosas. Las plataformas deben mostrar los precios en moneda de curso legal, establecer límites de gasto y solicitar confirmaciones adicionales. La apariencia lúdica

de una transacción no elimina su posible impacto económico sobre el menor y su familia.

El diseño persuasivo puede prolongar innecesariamente la conexión mediante recompensas, notificaciones, eventos limitados o penalizaciones por abandonar una sesión. Estas prácticas pueden afectar descanso, concentración, estudio y relaciones familiares. El interés superior exige evaluar si la arquitectura explota vulnerabilidades vinculadas con la edad. Los controles familiares son útiles, pero no sustituyen la responsabilidad del proveedor. Las plataformas deben incorporar pausas, recordatorios y opciones para desactivar estímulos, evitando que su modelo económico dependa de mantener al menor conectado durante periodos excesivos.

Los espacios educativos requieren precauciones adicionales porque la participación puede ser obligatoria. Una institución no debería exigir datos biométricos, emocionales o conductuales que no sean indispensables para alcanzar el objetivo pedagógico. Peña y Rubio (2024) destacan la necesidad de integrar las tecnologías inmersivas mediante criterios éticos, inclusivos y adecuados al contexto educativo. Estudiantes y representantes deben conocer si las sesiones serán grabadas, quién tendrá acceso, cuánto tiempo se conservarán los registros y si los datos se utilizarán para evaluar el rendimiento.

La protección frente a contenidos perjudiciales debe equilibrarse con el derecho del menor a la educación, cultura, información y participación. La Constitución de la República del Ecuador (2008), artículo 46, numeral 7, exige medidas frente a mensajes que promuevan violencia o discriminación. Sin embargo, los filtros no deberían bloquear indiscriminadamente contenidos educativos, artísticos o informativos. La moderación debe considerar contexto, edad y finalidad, combinando herramientas automatizadas con intervención humana para reducir tanto la exposición dañina como las restricciones injustificadas.

2.6 Suplantación de identidad digital

La suplantación de identidad digital en el metaverso consiste en utilizar sin autorización datos, credenciales, rasgos personales o representaciones virtuales para aparentar ser otra persona. Puede producirse mediante el acceso ilegítimo a una cuenta, la copia de un avatar, la imitación de la voz o la creación de una réplica hiperrealista. Sus consecuencias no se limitan al perjuicio económico, pues también pueden afectar la

intimidad, el honor, la reputación, las relaciones personales y la seguridad del titular suplantado (Castillo et al., 2024).

Los entornos inmersivos amplían las modalidades de suplantación porque la identidad se expresa mediante múltiples elementos simultáneos. El nombre, la apariencia, la voz, los movimientos, las credenciales y los objetos asociados con el avatar pueden formar una representación reconocible. Una persona puede ser identificada incluso cuando no utiliza su nombre civil. La valoración jurídica debe examinar el conjunto de atributos copiados y su capacidad para generar una percepción falsa sobre quién controla realmente la cuenta o representación virtual (Sorrentino y López, 2025).

La Constitución de la República del Ecuador (2008), artículo 66, numeral 28, reconoce el derecho a la identidad personal y colectiva, incluyendo características materiales e inmateriales que individualizan a una persona. Esta protección puede extenderse a las representaciones digitales vinculadas de manera estable con su titular. Aunque el avatar adopte rasgos ficticios, su uso constante, reputación y relaciones pueden convertirlo en parte relevante de la identidad digital. La apropiación ilegítima afecta la continuidad, autenticidad y control que la persona ejerce sobre su representación.

La suplantación debe diferenciarse de la representación ficticia, la parodia y la coincidencia accidental. Utilizar una apariencia semejante no constituye por sí mismo una vulneración. La conducta adquiere relevancia cuando existe intención de inducir a terceros a creer que interactúan con otra persona, obtener un beneficio, acceder a información o perjudicar su reputación. Deben analizarse la semejanza, el contexto, la finalidad, los contactos realizados y los actos posteriores. La evaluación no puede basarse únicamente en la coincidencia de nombres o accesorios virtuales.

Una primera modalidad es la apropiación de cuenta, que ocurre cuando un tercero obtiene contraseñas, códigos, dispositivos o credenciales y accede al perfil legítimo. En este caso, el infractor controla la identidad ya consolidada, incluidos contactos, activos, conversaciones y antecedentes. Fiaz et al. (2024) señalan que los sistemas de identidad digital requieren mecanismos reforzados de autenticación y control. La plataforma debe detectar accesos anómalos, permitir el cierre remoto de sesiones y facilitar procedimientos de recuperación sin exigir información desproporcionada.

Otra modalidad es la clonación externa del avatar, en la cual se crea una nueva cuenta que reproduce nombre, apariencia, voz o comportamiento sin controlar la original. Esta

práctica puede utilizarse para contactar a familiares, colegas, clientes o comunidades y generar confianza. Castillo et al. (2024) explican que las herramientas de personalización incrementan la capacidad para crear representaciones convincentes. Las plataformas deben permitir comparar perfiles, verificar fechas de creación y analizar si la similitud responde a una coincidencia legítima o a una estrategia deliberada de engaño.

La inteligencia artificial generativa facilita la imitación de rostros, voces y gestos. Una réplica puede participar en reuniones, solicitar transferencias, obtener información confidencial o difundir declaraciones falsas con una apariencia de autenticidad. Sorrentino y López (2025) advierten que los datos biométricos e inferidos utilizados por los entornos inmersivos aumentan la posibilidad de reproducir identidades. La verificación no debería depender únicamente de la imagen o la voz, especialmente en operaciones patrimoniales, profesionales o institucionales de alto riesgo.

La LOPDP (2021), artículo 4, resulta aplicable cuando se utilizan nombres, rostros, voces, movimientos o perfiles capaces de identificar a una persona. La recopilación y reproducción de estos atributos constituye tratamiento de datos y necesita una base legitimadora. La disponibilidad pública de una fotografía o grabación no autoriza su utilización para crear una identidad falsa. Cuando intervienen datos biométricos, el riesgo aumenta porque están estrechamente vinculados con el cuerpo y no pueden reemplazarse con la facilidad de una contraseña.

La suplantación puede afectar simultáneamente el honor, el buen nombre, la imagen y la voz. La Constitución de la República del Ecuador (2008), artículo 66, numeral 18, protege estos derechos. Crear un avatar que publique expresiones ofensivas, realice actos reprochables o difunda información falsa atribuida al titular puede perjudicar su reputación. El daño se intensifica cuando el contenido circula fuera de la plataforma o alcanza espacios familiares, profesionales y académicos. El retiro debe complementarse con medidas de rectificación cuando la falsedad ya produjo consecuencias.

Figura 6
Modalidades de suplantación de identidad digital



Nota. La figura presenta las principales modalidades de suplantación de identidad digital: apropiación de cuentas, clonación de avatares e imitación mediante inteligencia artificial. Elaboración propia**.**

En el ámbito penal, la suplantación no establece automáticamente un delito autónomo por el simple uso de una identidad ajena. La calificación depende de las conductas realizadas y de su adecuación a los tipos previstos en el COIP (2014). Pueden resultar relevantes la estafa, la apropiación fraudulenta por medios electrónicos, el acceso no consentido a sistemas o la interceptación ilegal de datos. El principio de legalidad exige comprobar cada elemento del delito, la intención del responsable y la relación entre la identidad simulada y el resultado producido.

Varela et al. (2025) destacan que la inteligencia artificial amplía las capacidades de la ciberdelincuencia y dificulta la detección de contenidos falsificados. Esta evolución exige investigar no solo el perfil visible, sino también los registros de acceso, dispositivos, aplicaciones y herramientas utilizadas. La dirección IP o el correo asociado constituyen indicios, pero no demuestran por sí solos la autoría, pues pueden pertenecer a cuentas comprometidas, redes compartidas o servicios intermediarios. La atribución debe construirse mediante un conjunto coherente de evidencias.

Las plataformas poseen deberes de diligencia cuando reciben una denuncia fundada. No se les exige impedir absolutamente toda imitación, pero sí disponer de canales accesibles, analizar oportunamente la información y limitar la continuidad del daño. La respuesta no debería consistir en eliminar automáticamente cualquier perfil parecido,

porque varias personas pueden compartir nombres o características. Deben valorarse la intención de engaño, los mensajes enviados, las solicitudes económicas, la copia de contenidos y la relación con la identidad denunciada.

Los procedimientos de verificación deben respetar el principio de minimización. Una víctima no debería entregar copias completas de documentos, datos biométricos o información innecesaria para recuperar su identidad. La plataforma puede utilizar el historial de la cuenta, canales previamente registrados, comprobantes de creación o validaciones institucionales. Los documentos adicionales deben solicitarse únicamente cuando sean indispensables, protegerse mediante medidas de seguridad y eliminarse una vez cumplida su finalidad, conforme a los principios establecidos en la LOPDP (2021), artículo 10.

La prevención debe combinar autenticación, educación y diseño tecnológico. La autenticación multifactor, las alertas de acceso, los límites transaccionales y los identificadores verificables reducen determinados riesgos. Sin embargo, exigir biometría obligatoria a todos los usuarios puede resultar desproporcionado. Fiaz et al. (2024) proponen modelos de identidad que aumentan el control del titular, pero cualquier solución debe ofrecer alternativas accesibles. La seguridad no debe convertirse en una forma permanente de vigilancia ni concentrar toda la identidad en una única credencial vulnerable.

Los menores requieren medidas reforzadas porque pueden tener mayores dificultades para reconocer avatares falsos o voces sintéticas. Un adulto puede simular ser un compañero, una figura de confianza o una institución educativa para obtener información, imágenes o acceso a espacios privados. La Constitución de la República del Ecuador (2008), artículos 44 y 45, exige priorizar su interés superior, identidad e integridad. Las plataformas deben restringir contactos sospechosos, ofrecer alertas comprensibles y facilitar la intervención de moderadores especializados.

La preservación de evidencia resulta indispensable para investigar la suplantación. Deben conservarse de forma restringida identificadores, mensajes, registros de acceso, archivos sintéticos y transacciones relacionadas con el incidente. La víctima puede aportar capturas y fechas, procurando no difundir públicamente datos de terceros o contenidos íntimos. La plataforma debe impedir la alteración o eliminación inmediata

de los registros relevantes cuando exista una reclamación fundada. Esta conservación debe limitarse al tiempo necesario y sujetarse a controles de confidencialidad.

La reparación debe adaptarse a las consecuencias producidas. Puede incluir recuperación de la cuenta, retiro de la réplica, restitución de activos, corrección de perfiles, anulación de sanciones y comunicación a las personas engañadas. La LOPDP (2021), artículos 14 y 15, permite solicitar rectificación y eliminación de información inexacta o tratada ilegítimamente. Si las conductas del suplantador fueron atribuidas a la víctima, deben corregirse también los historiales, puntuaciones y decisiones automatizadas que continúen utilizando esos antecedentes falsos.

2.7 Hábeas data y tutela digital

El hábeas data constituye una garantía jurisdiccional destinada a proteger el control de las personas sobre la información que las identifica o se relaciona con sus bienes. Su relevancia aumenta en el metaverso porque las plataformas pueden recopilar voz, rostro, movimientos, conversaciones, transacciones y patrones de conducta. Estos datos no solo permiten autenticar al usuario, sino también elaborar perfiles, inferir preferencias y adoptar decisiones automatizadas. La tutela debe abarcar tanto la información entregada directamente como aquella observada o generada durante la experiencia inmersiva (Tukur et al., 2023).

La Constitución de la República del Ecuador (2008), artículo 92, reconoce el derecho de toda persona a conocer la existencia y acceder a documentos, datos genéticos, bancos o archivos de información personal e informes sobre sí misma o sus bienes. También permite conocer el uso, finalidad, origen, destino y tiempo de vigencia de los datos. En el metaverso, esta garantía puede dirigirse contra plataformas, fabricantes de dispositivos, desarrolladores, proveedores de almacenamiento y otras entidades públicas o privadas que administren información vinculada con usuarios identificados o identificables.

El hábeas data no debe limitarse a entregar una copia del nombre, correo electrónico o información visible del perfil. La tutela debe comprender registros internos, historiales de interacción, puntuaciones, perfiles conductuales e inferencias utilizadas para personalizar contenidos o adoptar decisiones. Fernandez y Hui (2022) advierten que los entornos inmersivos permiten reconstruir aspectos profundos de la conducta mediante

la combinación de señales corporales y digitales. Una respuesta fragmentaria impediría conocer la verdadera dimensión del tratamiento y sus posibles efectos sobre el titular.

El derecho a la información constituye una condición previa para ejercer cualquier otra facultad. La LOPDP (2021), artículo 12, permite conocer las finalidades, la base legitimadora, las categorías de datos, el tiempo de conservación, las transferencias y los mecanismos disponibles para ejercer derechos. En un entorno inmersivo, esta información debe presentarse de forma comprensible y contextual. La complejidad técnica no justifica descripciones ambiguas sobre sensores, algoritmos o inferencias, especialmente cuando pueden condicionar el acceso, la reputación, la visibilidad o las oportunidades económicas del usuario.

El derecho de acceso, regulado en la LOPDP (2021), artículo 13, permite conocer y obtener los datos personales tratados por el responsable. En el metaverso, debería comprender información declarada, registros de actividad, datos corporales, historiales de decisiones y perfiles inferidos. No resulta suficiente entregar archivos técnicos incomprensibles. La plataforma debe explicar su significado, la finalidad para la que se utilizan y, cuando corresponda, los criterios relevantes de las valoraciones automatizadas. La protección de terceros puede exigir ocultar algunos elementos, pero no negar completamente la información del solicitante.

La rectificación y actualización, reconocidas en la LOPDP (2021), artículo 14, permiten corregir información inexacta, incompleta o desactualizada. En los mundos virtuales, los errores pueden afectar la edad, identidad, titularidad de activos, historial disciplinario o autenticidad de una cuenta. También pueden surgir cuando las acciones de un suplantador se atribuyen al titular legítimo. La corrección debe extenderse a perfiles, puntuaciones y decisiones derivadas del dato falso; de lo contrario, las consecuencias de la inexactitud continuarían afectando al usuario incluso después de reconocerse el error.

El derecho de eliminación, previsto en la LOPDP (2021), artículo 15, permite solicitar la supresión cuando los datos dejan de ser necesarios, se tratan ilegítimamente o se cumplen otras condiciones legales. Esta facultad puede comprender registros biométricos, grabaciones, historiales de ubicación, copias de avatares y perfiles comerciales. Sin embargo, la eliminación no es absoluta cuando existe una obligación legítima de conservación. En esos casos, el responsable debe restringir el acceso y evitar

que la información continúe utilizándose para publicidad, recomendaciones o decisiones automatizadas.

Tabla 6
Aplicación del hábeas data frente a controversias del metaverso

Situación controvertida	Derecho o garantía aplicable	Información que debe entregar o corregir el responsable	Resultado esperado	Riesgo si no se atiende
Recopilación oculta de voz y movimientos	Información y acceso	Categorías, finalidad, destinatarios y plazo de conservación	Conocimiento integral del tratamiento	Vigilancia no advertida
Perfil conductual inexacto	Rectificación y actualización	Variables utilizadas, inferencias y decisiones derivadas	Corrección del perfil y sus efectos	Discriminación o restricción
Conservación indefinida de biometría	Eliminación	Justificación, plazo y necesidad del registro	Supresión o restricción fundada	Exposición permanente
Seguimiento comercial entre plataformas	Oposición	Finalidad, base jurídica y terceros involucrados	Cese del perfilamiento cuando corresponda	Manipulación y pérdida de control
Suspensión automatizada de una cuenta	Revisión de decisiones	Regla aplicada, datos relevantes y nivel de intervención humana	Explicación y revisión efectiva	Exclusión arbitraria
Suplantación atribuida al titular	Rectificación y reparación	Accesos, operaciones y sanciones vinculadas	Corrección de antecedentes	Daño reputacional continuado
Traslado de datos a otro entorno	Portabilidad	Datos transferibles y formato disponible	Entrega segura y estructurada	Dependencia de la plataforma
Negativa injustificada de acceso	Hábeas data jurisdiccional	Archivo completo y fundamentos de la negativa	Orden judicial de acceso o corrección	Indefensión del titular
Uso de datos de menores	Tutela reforzada	Finalidades, autorizaciones y medidas aplicadas	Restricción o eliminación prioritaria	Afectación al interés superior

Situación controvertida	Derecho o garantía aplicable	Información que debe entregar o corregir el responsable	Resultado esperado	Riesgo si no se atiende
Conservación de evidencia de un incidente	Limitación y seguridad	Alcance, acceso y plazo de custodia	Preservación restringida	Exposición innecesaria

Nota. La garantía aplicable depende de la finalidad del tratamiento, la exactitud de la información y la existencia de una causa jurídica que justifique su conservación.

El derecho de oposición adquiere importancia frente al seguimiento conductual y publicitario. El usuario puede cuestionar la observación entre plataformas, el análisis emocional o la personalización invasiva cuando concurran las condiciones previstas por la legislación. La respuesta del responsable debe valorar la situación concreta y no limitarse a invocar genéricamente la mejora del servicio. Fernandez y Hui (2022) destacan que la recopilación continua incrementa la capacidad de vigilancia y reutilización, por lo que el titular necesita mecanismos efectivos para limitar tratamientos que no resulten indispensables.

La portabilidad puede fortalecer el control del usuario y reducir la dependencia respecto de una sola plataforma. Esta facultad permite recibir determinados datos en un formato estructurado y trasladarlos a otro proveedor. No obstante, debe distinguirse entre información personal, componentes licenciados, contenidos de terceros y activos sometidos a reglas diferentes. Smith et al. (2025) señalan que la interoperabilidad plantea dificultades jurídicas relacionadas con reconocimiento, control y transferencia. La portabilidad de datos no equivale automáticamente a trasladar todos los elementos del avatar o del patrimonio virtual.

Las decisiones automatizadas constituyen uno de los principales escenarios de tutela digital. La LOPDP (2021), artículo 20, reconoce garantías frente a valoraciones automatizadas que producen efectos jurídicos o afectan derechos y libertades. Una plataforma puede suspender cuentas, limitar contenidos, restringir espacios o calificar a un usuario como riesgoso. El afectado debe conocer los factores relevantes y solicitar intervención humana. Una explicación basada únicamente en la existencia de actividad inusual no permite comprender el supuesto incumplimiento ni preparar una impugnación adecuada.

La revisión humana debe ser sustancial y estar a cargo de una persona con capacidad para modificar el resultado. Los sistemas pueden interpretar incorrectamente acentos,

discapacidades, gestos, movimientos o expresiones culturales. La tutela efectiva exige acceder a la información utilizada, cuestionar inferencias y demostrar errores contextuales. Una revisión que simplemente confirme el resultado algorítmico no satisface la finalidad protectora del procedimiento.

La Sentencia 182-15-SEP-CC (2015) de la Corte Constitucional del Ecuador resulta pertinente para reforzar el acceso y control de la información personal. Su aplicación permite sostener que el titular no depende únicamente de la voluntad contractual de la plataforma para conocer o corregir los datos que le conciernen. Los procedimientos internos pueden facilitar el ejercicio de derechos, pero no sustituyen la garantía jurisdiccional cuando existe una negativa, respuesta incompleta o incumplimiento. El control sobre la información personal posee naturaleza constitucional y debe ser efectivamente tutelado.

La Sentencia 89-19-JD/21 (2021) también aporta criterios relevantes sobre el objeto y alcance del hábeas data. Esta jurisprudencia permite comprender que la garantía no se agota en la entrega material de archivos, sino que puede incluir actualización, rectificación, eliminación o anulación de información. En el metaverso, esta amplitud resulta necesaria cuando una clasificación, sanción o perfil incorrecto continúa produciendo consecuencias. La tutela debe dirigirse tanto contra el dato erróneo como contra los efectos derivados de su utilización en sistemas automatizados o decisiones institucionales.

La Sentencia 47-19-JD/22 (2022) permite precisar que el derecho de acceso mediante hábeas data no es absoluto cuando el archivo contiene información perteneciente a terceras personas. La Corte diferenció los datos personales de la persona denunciada de aquellos correspondientes a quien presentó la denuncia. En el metaverso, esta distinción resulta aplicable cuando una solicitud de acceso involucra conversaciones, reportes o expedientes que contienen información de varios usuarios. La plataforma debe entregar los datos del solicitante y proteger, anonimizar o restringir aquellos pertenecientes a terceros.

La LOGJCC (2009), artículos 49 a 51, regula el objeto, procedencia y legitimación de la acción de hábeas data. Esta vía puede activarse cuando el responsable niega el acceso, no corrige información inexacta, conserva datos sin justificación o incumple una solicitud legítima de eliminación. En el metaverso, la acción permite superar la

dependencia de formularios internos diseñados unilateralmente por la plataforma. La ubicación extranjera del servidor no elimina automáticamente la protección cuando el tratamiento se vincula con residentes ecuatorianos o produce efectos dentro del país.

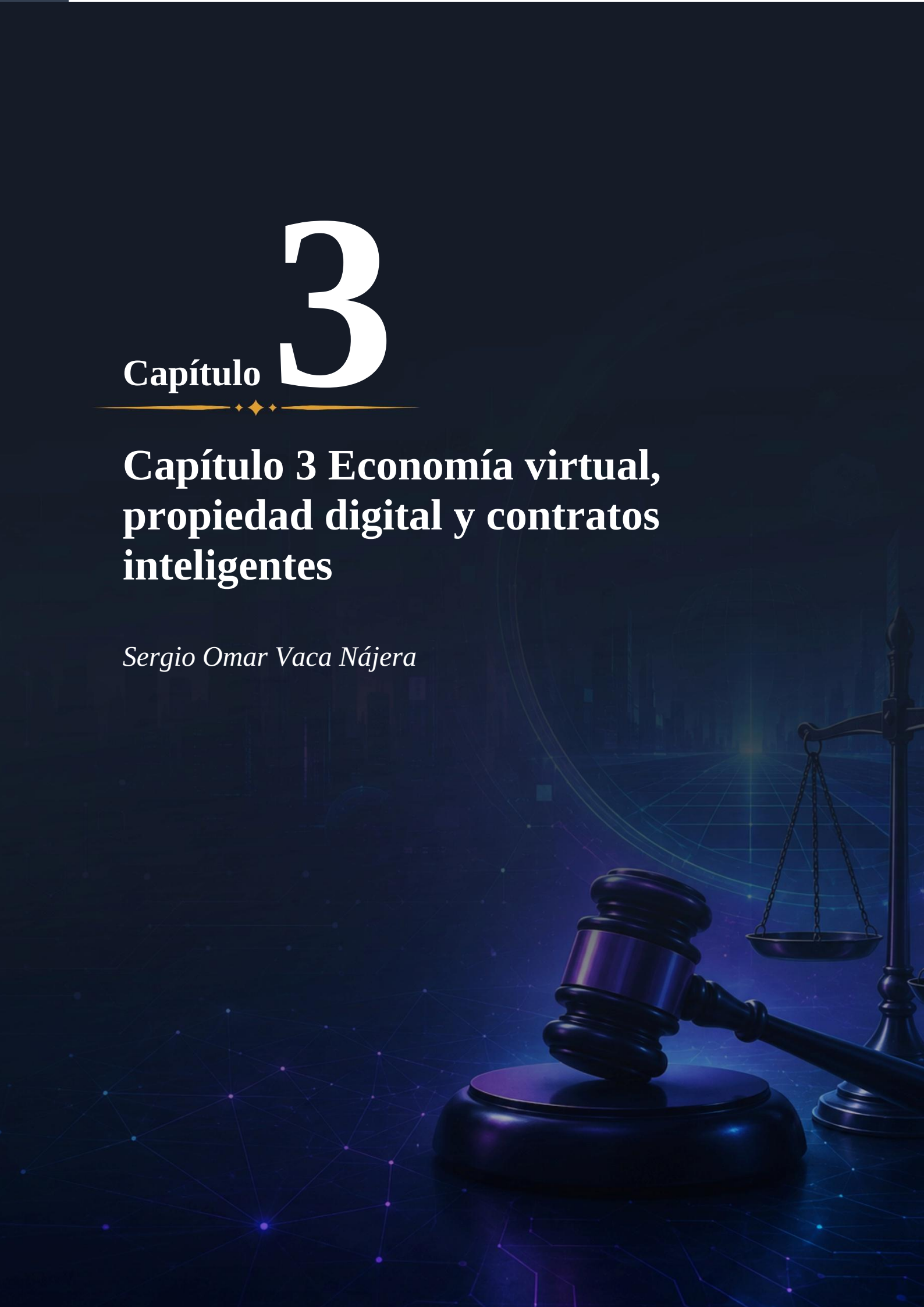
La tutela digital debe considerar la rapidez con la que la información puede copiarse, difundirse o incorporarse a sistemas automatizados. Una respuesta tardía puede resultar inútil cuando una réplica continúa circulando, una clasificación impide utilizar servicios o una sanción afecta actividades profesionales. La preservación de evidencia no exige mantener públicamente el contenido perjudicial. La plataforma puede retirarlo de circulación y conservar una copia restringida, aplicando finalidad, proporcionalidad, confidencialidad y seguridad durante el tiempo estrictamente necesario para resolver la controversia.

Las niñas, niños y adolescentes necesitan procedimientos simplificados y compatibles con su autonomía progresiva. La Constitución de la República del Ecuador (2008), artículos 44 y 45, y el Código de la Niñez y Adolescencia (2003), artículo 53, protegen su identidad, intimidad y comunicaciones. Una solicitud relacionada con su información no debería exigir formularios complejos ni una exposición adicional de datos. La plataforma debe priorizar la corrección, retiro o restricción cuando existan suplantaciones, contactos indebidos, difusión de contenidos íntimos o perfiles perjudiciales.

Capítulo 3

Capítulo 3 Economía virtual, propiedad digital y contratos inteligentes

Sergio Omar Vaca Nájera



3.1 Economía del metaverso

La economía del metaverso comprende las actividades de producción, intercambio, consumo y generación de valor desarrolladas dentro de entornos virtuales persistentes. En estos espacios, los participantes pueden adquirir bienes digitales, contratar servicios, crear contenidos, organizar eventos o recibir remuneraciones mediante monedas internas y otros mecanismos de pago. Su particularidad radica en que una misma persona puede actuar simultáneamente como usuaria, consumidora, creadora y proveedora. Esta convergencia amplía las oportunidades comerciales, pero también dificulta identificar la naturaleza jurídica de cada operación (Jauhiainen et al., 2023).

Los modelos económicos pueden ser centralizados, descentralizados o híbridos. En los sistemas centralizados, la empresa operadora controla la emisión de monedas internas, las reglas del mercado, la permanencia de los activos y el acceso de los participantes. En los modelos descentralizados, algunas operaciones utilizan cadenas de bloques, tokens o contratos inteligentes para registrar transferencias. Madanchian y Taherdoost (2024) advierte que la evolución de estos modelos depende de la confianza, la utilidad y la sostenibilidad del ecosistema, sin que la descentralización elimine la intervención de actores con capacidad de decisión económica.

La creación de contenidos por los usuarios constituye uno de los principales motores de la economía virtual. Los participantes pueden diseñar accesorios, escenarios, obras, experiencias educativas, servicios profesionales y herramientas para otros usuarios. Esta actividad transforma al consumidor tradicional en productor y genera nuevas formas de emprendimiento. No obstante, también plantea interrogantes sobre autoría, remuneración, licencias y distribución de ingresos. Las plataformas deben informar si el creador conserva sus derechos, concede una autorización limitada o permite determinados usos comerciales de su producción (Kostenko et al., 2022).

Las monedas internas facilitan el intercambio dentro de determinados ecosistemas. Pueden utilizarse para adquirir objetos, acceder a servicios, recompensar actividades o remunerar creaciones. Sin embargo, su denominación comercial no determina que constituyan dinero de curso legal ni garantiza su conversión en moneda oficial. El valor puede depender completamente de las reglas del proveedor, quien podría modificar tasas, limitar retiros o cerrar el mercado. La plataforma debe informar sobre

convertibilidad, vigencia, restricciones de uso y condiciones para recuperar saldos (Kasiyanto y Kilinc, 2022).

La escasez digital influye en la formación del valor cuando un objeto se presenta como exclusivo, limitado o único mediante restricciones técnicas, decisiones empresariales o registros distribuidos. Esa escasez debe ser verificable y explicarse con claridad, porque el proveedor puede conservar la facultad de emitir nuevas versiones, modificar funcionalidades o retirar la utilidad asociada. Madanchian y Taherdoost (2024) relaciona el valor de estos activos con la confianza, la comunidad y la sostenibilidad del modelo de negocio, además de su disponibilidad técnica.

La participación económica puede incluir además prestación de servicios profesionales, actividades educativas, diseño, entretenimiento, publicidad y organización de eventos. Un usuario puede recibir pagos por asesorías, presentaciones, creación de espacios o venta de contenidos. Estas relaciones no pierden su naturaleza económica por ejecutarse mediante avatares. Deben identificarse el prestador, el destinatario, la contraprestación y las condiciones del servicio. La apariencia virtual puede facilitar la interacción, pero no sustituye la necesidad de determinar quién asume obligaciones y responde frente a incumplimientos.

La economía virtual también presenta riesgos derivados del cierre o transformación de la plataforma. Un activo puede perder utilidad cuando el proveedor descontinúa el servicio, modifica sus reglas o deja de reconocer determinados objetos. La persistencia tecnológica no garantiza continuidad económica. Jauhiainen et al. (2023) advierten que la estabilidad de los ecosistemas depende de decisiones empresariales y condiciones de sostenibilidad. Los participantes deben conocer anticipadamente si existen mecanismos de exportación, reembolso, conversión de saldos o recuperación de contenidos.

La participación de menores exige salvaguardas reforzadas cuando los bienes se presentan como recompensas, elementos de estatus o condiciones para avanzar dentro de una experiencia. Las monedas internas pueden dificultar la comprensión del costo real, mientras los mecanismos de escasez o presión grupal pueden fomentar compras impulsivas. Las plataformas deben incorporar límites de gasto, confirmaciones adicionales e información adecuada para la edad. La apariencia lúdica de la operación no elimina su impacto económico ni la obligación de proteger el interés superior del menor.

La economía del metaverso también puede generar desigualdades. El acceso a determinados espacios, herramientas o experiencias puede depender de pagos, dispositivos costosos o conectividad avanzada. Jauhiainen et al. (2023) señalan que los mundos virtuales pueden reproducir exclusiones existentes cuando sus modelos económicos privilegian a quienes poseen mayores recursos. La sostenibilidad de estos entornos requiere valorar no solo rentabilidad y crecimiento, sino también accesibilidad, distribución de beneficios y condiciones justas para quienes producen contenidos o prestan servicios.

La economía del metaverso debe analizarse como un sistema en el que convergen creación, consumo, intercambio y tratamiento de datos. Su regulación no puede depender únicamente de la tecnología utilizada ni de las denominaciones comerciales adoptadas por las plataformas. Es necesario identificar qué derecho adquiere el usuario, qué obligaciones asume el proveedor y qué riesgos surgen del diseño de la experiencia. La transparencia, la protección del consumidor y la claridad contractual constituyen condiciones esenciales para una participación económica jurídicamente segura (Jauhiainen et al., 2023; Madanchian y Taherdoost, 2024).

3.2 Bienes y activos digitales

Los bienes y activos digitales establecen elementos centrales de la economía del metaverso porque representan utilidades, contenidos y posiciones con posible valor económico dentro de los entornos virtuales. Esta categoría puede comprender accesorios para avatares, terrenos virtuales, entradas, herramientas, monedas internas, obras digitales y derechos de acceso. Aunque carezcan de materialidad física, pueden ser objeto de intercambio y producir expectativas patrimoniales. Su análisis jurídico debe atender a la función concreta del elemento, las facultades otorgadas al usuario y las condiciones establecidas por la plataforma (Kostenko et al., 2022).

La expresión bien digital puede utilizarse para describir cualquier recurso creado, almacenado o utilizado mediante sistemas informáticos. El término activo digital suele destacar que ese recurso posee valor, puede transferirse o genera una ventaja económica. No obstante, la diferencia no siempre es absoluta. Un mismo objeto puede cumplir una función estética, social, funcional y patrimonial. Una prenda virtual, por ejemplo, puede personalizar un avatar, expresar pertenencia comunitaria y, al mismo

tiempo, ser revendida dentro de un mercado autorizado por la plataforma (Madanchian y Taherdoost, 2024).

Los activos virtuales pueden clasificarse según su función. Los activos utilitarios habilitan herramientas, espacios o servicios; los representativos acreditan una posición, entrada o credencial; los ornamentales modifican la apariencia del usuario; y los consumibles desaparecen después de ser utilizados. También existen activos persistentes que permanecen vinculados a una cuenta y elementos transferibles que pueden circular entre usuarios. Esta clasificación permite comprender mejor las expectativas del adquirente y determinar qué consecuencias deben producir la pérdida, modificación o eliminación del recurso digital (Kasiyanto y Kilinc, 2022).

La adquisición de un activo digital puede adoptar diferentes formas jurídicas. En algunos casos, el usuario obtiene una licencia para utilizarlo dentro de una plataforma; en otros, adquiere un derecho de acceso, una prestación pendiente o una facultad de transferencia. La denominación empleada por el proveedor no es suficiente para establecer la naturaleza del negocio. Expresiones como compra, propiedad o posesión deben compararse con las condiciones reales de uso. Martínez et al. (2024) destacan que la calificación depende de las facultades efectivamente reconocidas al participante.

La infraestructura tecnológica influye directamente en el control del activo. En plataformas centralizadas, el proveedor administra cuentas, bases de datos y permisos, por lo que puede modificar o retirar elementos mediante decisiones internas. En sistemas basados en cadenas de bloques, el usuario puede controlar una clave que permite transferir un token. Sin embargo, ambos modelos pueden imponer restricciones jurídicas o técnicas. Martínez et al. (2024) señalan que la descentralización modifica la forma de administración, pero no elimina contratos, licencias ni responsabilidades.

La transferibilidad determina si el usuario puede vender, regalar o trasladar un activo. Algunos elementos permanecen vinculados a una cuenta y no pueden circular, mientras otros cuentan con mercados secundarios. La posibilidad técnica de transferir no implica que la operación esté libre de condiciones. Pueden existir comisiones, restricciones territoriales, límites de uso o derechos de terceros. La plataforma debe informar estas condiciones antes de la adquisición, pues la expectativa de reventa puede influir considerablemente en la decisión económica del usuario (Kostenko et al., 2022).

La interoperabilidad añade otra dimensión al análisis. Un activo puede funcionar correctamente dentro de una plataforma y carecer de utilidad en otra debido a diferencias de formato, diseño o licencias. La promesa de trasladar objetos entre mundos virtuales debe distinguir entre compatibilidad técnica y reconocimiento jurídico. Un sistema puede importar el archivo sin aceptar las mismas facultades de modificación o comercialización. Tukur et al. (2023) sostienen que la portabilidad exige coordinación entre estándares, contratos y derechos vinculados con cada recurso digital.

Tabla 7
Clasificación funcional y jurídica de bienes y activos digitales

Tipo de activo	Función principal	Derecho o interés posible	Riesgo predominante
Accesorio para avatar	Personalización e identidad	Licencia de uso	Retiro o modificación unilateral
Terreno virtual	Construcción o reunión	Acceso exclusivo o uso contractual	Confusión con propiedad inmobiliaria
Moneda interna	Intercambio dentro de la plataforma	Saldo frente al proveedor	Devaluación o bloqueo
Entrada virtual	Acceso a evento o experiencia	Derecho a recibir un servicio	Cancelación o prestación defectuosa
Herramienta digital	Habilitación de funciones	Uso temporal o permanente	Pérdida de funcionalidad
Obra digital	Expresión y comercialización	Derecho de autor y licencia	Reproducción no autorizada
Token	Registro o representación digital	Control técnico y facultad contractual	Confusión sobre derechos subyacentes
Credencial virtual	Identificación o acreditación	Reconocimiento institucional	Falsificación o revocación
Activo consumible	Uso único dentro del entorno	Prestación agotable	Cobro o desaparición no comprendida
Activo transferible	Reventa o intercambio	Facultad de disposición limitada	Fraude y restricciones ocultas

Nota. La categoría comercial del activo debe diferenciarse de los derechos jurídicos realmente adquiridos por el usuario.

Los terrenos virtuales merecen una atención particular porque suelen representarse mediante parcelas, edificios o espacios delimitados. Esta apariencia puede generar la impresión de que funcionan como inmuebles, pero jurídicamente suelen consistir en permisos o facultades contractuales dentro de una plataforma. No existe suelo físico ni inscripción inmobiliaria tradicional. El usuario puede construir, organizar eventos o

restringir accesos según las reglas del sistema. La valoración jurídica debe concentrarse en la estabilidad, duración y alcance del derecho concedido, evitando analogías automáticas con la propiedad territorial.

Las monedas internas constituyen activos funcionales utilizados para adquirir bienes o servicios dentro de un ecosistema. Su valor puede ser fijado por el proveedor y no siempre existe posibilidad de conversión en moneda oficial. El usuario puede mantener un saldo, pero su disponibilidad depende de las condiciones de la plataforma. Madanchian y Taherdoost (2024) señala que estos sistemas forman parte de nuevos modelos de negocio virtuales. La información debe precisar si el saldo expira, puede retirarse, transferirse o perderse tras la suspensión de la cuenta.

La custodia de activos plantea riesgos relacionados con contraseñas, cuentas y claves criptográficas. En plataformas centralizadas, la recuperación puede depender del proveedor, mientras en sistemas descentralizados la pérdida de una clave puede impedir definitivamente el acceso. También pueden producirse transferencias fraudulentas mediante engaño o apropiación de credenciales. Fiaz et al. (2024) advierten que la irreversibilidad técnica no excluye la existencia de fraude o error. Los sistemas deben combinar seguridad, verificación y mecanismos proporcionales de reclamación o recuperación.

3.3 Propiedad de bienes virtuales

La propiedad de bienes virtuales constituye uno de los problemas jurídicos más complejos del metaverso porque la apariencia de control no siempre coincide con la titularidad reconocida por el derecho. Un usuario puede utilizar, modificar o transferir un objeto dentro de una plataforma sin ser propietario del archivo, del código o de la obra incorporada. La calificación depende del contrato, la arquitectura tecnológica y las facultades efectivamente concedidas. La expresión propiedad virtual debe emplearse con cautela y no como equivalente automático del dominio tradicional (Kostenko et al., 2022).

El punto de partida consiste en diferenciar entre control técnico y propiedad jurídica. El control técnico permite acceder, utilizar o transferir un activo mediante una cuenta, permiso o clave criptográfica. La propiedad jurídica, en cambio, supone un conjunto de facultades reconocidas y protegidas por el ordenamiento. Una persona puede controlar temporalmente un objeto sin poseer legitimidad para disponer de él, como ocurre

cuando se apropia de credenciales ajenas. Kasiyanto y Kilinc (2022) advierten que la tecnología registra operaciones, pero no determina por sí sola su validez.

El Código Civil (2005) distingue entre bienes corporales e incorporales. Su artículo 583 establece que los bienes consisten en cosas corporales o incorporales, mientras el artículo 594 relaciona estas últimas con derechos reales o personales. Esta clasificación permite aproximarse a los bienes virtuales, aunque no los convierte automáticamente en cosas susceptibles de dominio. En muchos casos, el interés del usuario se configura como un derecho contractual frente al proveedor, una licencia de uso o una posición económica dependiente del funcionamiento de la plataforma.

La Constitución de la República del Ecuador (2008), artículo 66, numeral 26, reconoce el derecho a la propiedad en todas sus formas, mientras el artículo 321 garantiza distintas modalidades de propiedad conforme a su función social y ambiental. Estas disposiciones permiten proteger intereses patrimoniales surgidos en entornos digitales. Sin embargo, la tutela constitucional no elimina la necesidad de determinar qué derecho adquirió realmente el usuario. La existencia de valor económico o exclusividad técnica no basta para concluir que existe propiedad plena sobre el objeto virtual.

La propiedad virtual puede manifestarse mediante diferentes estructuras. En algunos casos, el usuario obtiene una licencia revocable; en otros, una facultad de uso permanente mientras exista la plataforma. También puede adquirir un derecho de acceso, una autorización de transferencia o el control de un token. Kostenko et al. (2022) señalan que la naturaleza jurídica debe identificarse según las facultades concretas de uso, exclusión, modificación, transmisión y aprovechamiento económico. La denominación comercial del activo no sustituye este análisis funcional.

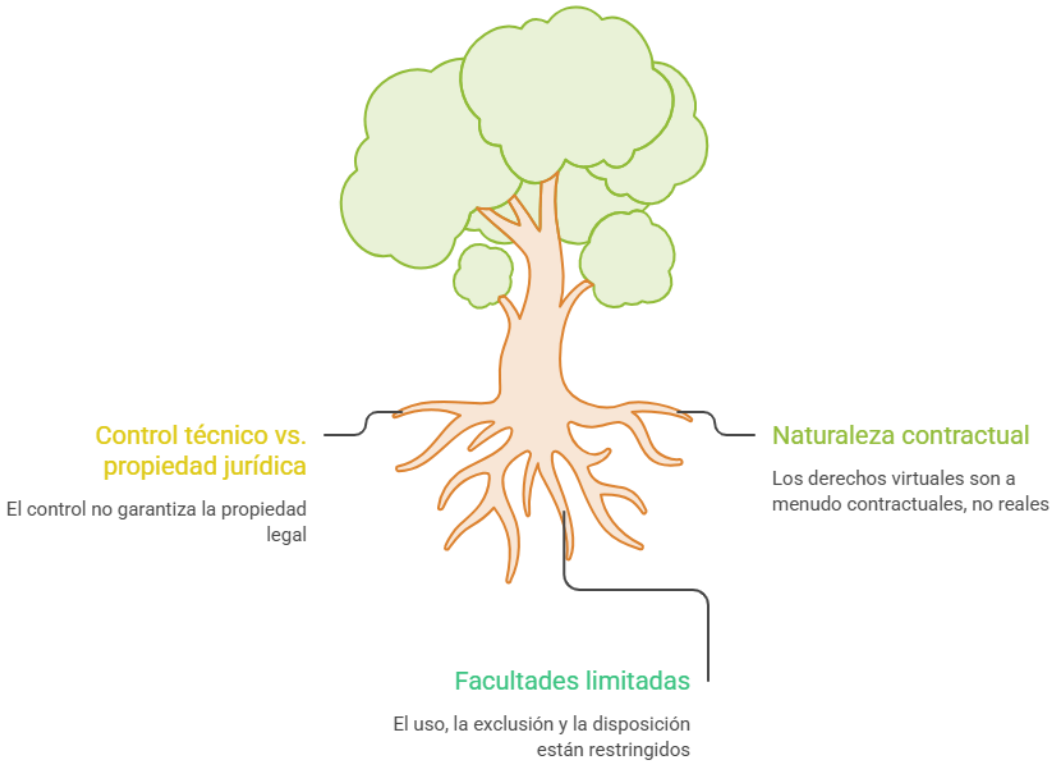
La facultad de uso permite emplear el bien dentro de las condiciones autorizadas. Puede comprender vestir un avatar, ingresar a un espacio, utilizar una herramienta o exhibir una obra. La amplitud del uso depende de la licencia y de las reglas técnicas. Un objeto puede estar limitado a una cuenta, dispositivo o plataforma. Si el proveedor conserva la posibilidad de restringir unilateralmente su utilización, debe informar esa circunstancia. El usuario necesita conocer si el uso es temporal, indefinido, exclusivo, compartido o condicionado al mantenimiento del servicio.

La facultad de exclusión permite impedir que otros utilicen o accedan al bien. En entornos virtuales, esta capacidad depende frecuentemente del código y de los permisos

administrados por la plataforma. Un terreno virtual puede configurarse como privado, pero el operador conserva control sobre servidores, accesos y reglas. La exclusividad técnica no equivale necesariamente a un derecho real oponible frente a todos. Kasiyanto y Kilinc (2022) explican que la estructura tecnológica puede simular facultades propias de la propiedad sin reproducir completamente sus efectos jurídicos.

La facultad de disposición comprende vender, transferir, regalar o gravar un bien. Muchos activos virtuales no permiten libre disposición, porque permanecen vinculados a una cuenta o solo pueden intercambiarse en mercados autorizados. Incluso cuando existe transferencia técnica, pueden aplicarse comisiones, límites territoriales o restricciones derivadas de derechos intelectuales. El usuario debe conocer estas condiciones antes de adquirir el activo. La posibilidad de reventa puede constituir un elemento esencial de la decisión económica y no debe presentarse de manera ambigua.

Figura 7
Propiedad de bienes virtuales poco clara



Nota. La figura expone la falta de claridad jurídica sobre la propiedad de los bienes virtuales, debido al predominio del control técnico, la naturaleza contractual y las facultades limitadas del usuario. Elaboración propia.

La facultad de modificación depende de la licencia y de la naturaleza del bien. Algunos objetos pueden personalizarse, combinarse o transformarse, mientras otros permanecen técnicamente bloqueados. La modificación también puede afectar derechos del creador

o producir obras derivadas. Cuando la plataforma permite alterar un diseño, debe aclarar si esa autorización comprende únicamente el uso privado o también la explotación comercial. La libertad técnica para modificar un archivo no elimina las restricciones jurídicas derivadas del contrato o de la propiedad intelectual.

La estabilidad temporal del activo permite comprobar hasta qué punto la llamada propiedad virtual depende realmente del proveedor. Un bien puede permanecer durante años en una cuenta y desaparecer cuando la plataforma cierra, modifica su arquitectura o termina la relación contractual. Esta fragilidad demuestra que la exclusividad técnica no siempre produce una posición patrimonial equivalente al dominio sobre bienes físicos. Madanchian y Taherdoost (2024) vincula el valor de los activos digitales con la confianza en la continuidad del ecosistema; de ahí que el proveedor deba informar anticipadamente sobre respaldo, exportación, reembolso y recuperación.

Las reglas de la plataforma pueden afectar directamente el ejercicio de las facultades patrimoniales. Una suspensión puede impedir utilizar o transferir activos, mientras una actualización puede alterar su apariencia o funcionalidad. La Ley Orgánica de Defensa del Consumidor (2000) permite examinar cláusulas que autoricen modificaciones unilaterales perjudiciales o coloquen al usuario en indefensión. La aceptación de términos generales no legitima cualquier intervención sobre bienes adquiridos. Las decisiones deben apoyarse en causas claras, procedimientos previsibles y mecanismos de reclamación.

La titularidad no puede acreditarse mediante un solo registro técnico. Los comprobantes de compra, contratos, historiales de cuenta y operaciones distribuidas deben valorarse conjuntamente con el origen del activo, el consentimiento y la autenticación empleada. Una transferencia puede aparecer correctamente registrada y, sin embargo, proceder de credenciales sustraídas o de una cuenta comprometida. Como señalan Kasiyanto y Kilinc (2022), la trazabilidad facilita la reconstrucción de los hechos, pero no convierte automáticamente el control registrado en un derecho legítimo. La prueba exige relacionar la evidencia tecnológica con la causa jurídica de la adquisición.

La protección frente a terceros puede involucrar acciones contractuales, civiles, de consumo o propiedad intelectual. Si un usuario pierde acceso por incumplimiento del proveedor, la controversia puede ser contractual. Si otra persona utiliza ilegítimamente un activo, pueden existir daños o fraude. Cuando se reproduce una obra sin

autorización, intervienen derechos autorales. Esta diversidad confirma que no existe un único régimen de propiedad virtual. La respuesta depende de la naturaleza del bien, la conducta cuestionada y las facultades que correspondan al titular.

3.4 NFT y activos digitales

Los tokens no fungibles, conocidos como NFT, son registros digitales que permiten identificar de manera individualizada determinados activos dentro de una cadena de bloques. Su característica principal es la singularidad técnica del identificador, pues cada token contiene información que lo diferencia de otros. En el metaverso pueden vincularse con obras, accesorios, terrenos virtuales, entradas, credenciales o experiencias. Sin embargo, el NFT no debe confundirse con el contenido representado, ya que constituye un registro técnico cuya relevancia jurídica depende de los derechos efectivamente asociados (Martínez et al., 2024).

La no fungibilidad significa que el token no puede sustituirse automáticamente por otro idéntico, como ocurre con unidades monetarias equivalentes. Esta singularidad permite acreditar una posición dentro de un registro distribuido y seguir el historial de transferencias. No obstante, la individualización técnica no garantiza que el contenido vinculado sea único. Un mismo archivo puede reproducirse, almacenarse en diferentes servidores o relacionarse con varios tokens. Madanchian y Taherdoost (2024) advierte que la escasez digital depende tanto de la tecnología como de las reglas comerciales aplicadas por emisores y plataformas.

Para comprender jurídicamente un NFT deben distinguirse al menos cuatro elementos: el token, los metadatos, el archivo digital y los derechos subyacentes. El token contiene el identificador registrado; los metadatos describen el activo o incluyen un enlace; el archivo corresponde a la imagen, audio, modelo u obra; y los derechos subyacentes determinan qué puede hacer el adquirente. Martínez et al. (2024) señalan que confundir estos niveles genera expectativas equivocadas, especialmente cuando el comprador cree adquirir propiedad intelectual completa mediante la transferencia del token.

La adquisición de un NFT puede otorgar únicamente control técnico sobre el registro y la posibilidad de transferirlo. No atribuye automáticamente derechos de reproducción, modificación, distribución o explotación comercial del contenido asociado. Estas facultades deben constar expresamente en el contrato o licencia. El creador puede conservar todos los derechos de autor mientras el comprador obtiene una autorización

limitada para exhibir la obra. La plataforma debe explicar con claridad qué derecho se transmite y qué restricciones continúan vigentes después de la operación (Martínez et al., 2024).

La emisión de NFT puede utilizarse para representar accesorios de avatares, terrenos virtuales, entradas, certificados o membresías. En estos casos, el token cumple una función de acreditación dentro de un ecosistema. Su utilidad depende de que la plataforma reconozca el identificador y mantenga activa la función asociada. Kasiyanto y Kilinc (2022) sostienen que la tecnología distribuida puede facilitar trazabilidad y transferencia, pero la permanencia del beneficio continúa dependiendo de interfaces, desarrolladores y servicios capaces de interpretar el registro.

Los NFT también pueden integrarse en mercados secundarios, donde los titulares transfieren los tokens a otros usuarios. Esta circulación puede generar regalías automáticas para el creador, comisiones para la plataforma y beneficios para quienes adquieren y revenden. Sin embargo, la reventa no siempre garantiza ganancias ni liquidez. Madanchian y Taherdoost (2024) destaca que el valor depende de factores como reputación, demanda, utilidad, comunidad y sostenibilidad del proyecto. Presentar estos activos como inversiones seguras puede crear expectativas económicas engañosas.

La autenticidad constituye uno de los argumentos más utilizados para promover NFT. El registro puede demostrar que un token determinado fue emitido desde una dirección concreta y transferido mediante operaciones verificables. Sin embargo, no prueba necesariamente que quien lo emitió fuera el verdadero autor o titular del contenido. Una persona puede tokenizar una obra ajena o vincular un archivo utilizado sin autorización. Martínez et al. (2024) advierten que la trazabilidad técnica debe complementarse con verificación de autoría, licencia y legitimidad del emisor.

La inmutabilidad de la cadena de bloques tampoco garantiza la permanencia del archivo. En muchos casos, el token contiene únicamente un enlace hacia información almacenada fuera de la red. Si el servidor deja de funcionar, el contenido puede volverse inaccesible, aunque el token continúe registrado. Esta separación entre registro y archivo debe informarse antes de la adquisición. Kasiyanto y Kilinc (2022) explican que la descentralización puede coexistir con puntos centralizados de dependencia, especialmente en interfaces, almacenamiento y mercados de intercambio.

Tabla 8
Elementos jurídicos y tecnológicos asociados con los NFT

Elemento	Función principal	Derecho posible	Riesgo predominante
Token	Identifica una unidad dentro del registro	Control y transferencia técnica	Confusión con propiedad plena
Metadatos	Describen el activo vinculado	Información sobre contenido y emisión	Alteración o datos incompletos
Archivo digital	Contiene imagen, audio, modelo u obra	Uso sujeto a licencia	Pérdida o acceso interrumpido
Obra protegida	Expresión creativa incorporada	Derechos de autor	Tokenización sin autorización
Clave criptográfica	Permite controlar y transferir el token	Acceso técnico	Pérdida, robo o fraude
Contrato inteligente	Ejecuta transferencias y regalías	Automatización contractual	Error o ejecución irreversible
Mercado secundario	Facilita compraventa entre usuarios	Reventa condicionada	Volatilidad y manipulación
Plataforma	Permite visualizar y utilizar el NFT	Servicio de acceso	Cierre o suspensión
Licencia	Define facultades del adquirente	Uso, exhibición o explotación	Ambigüedad contractual
Registro distribuido	Conserva historial de operaciones	Evidencia técnica	Datos válidos con origen ilegítimo

Nota. El NFT constituye solo uno de los componentes de la operación y no incorpora automáticamente todos los derechos vinculados con el activo representado.

La pérdida o sustracción de una clave criptográfica puede provocar la transferencia no autorizada del token. Aunque la cadena registre la operación como válida, ello no significa que exista consentimiento legítimo. La irreversibilidad tecnológica puede dificultar la restitución, especialmente cuando el activo pasa por varias cuentas. Los sistemas deben incorporar autenticación reforzada, alertas y mecanismos de suspensión cuando existan indicios de fraude. La seguridad debe acompañar la trazabilidad y no confiar exclusivamente en la validez formal del registro.

Los NFT pueden ser objeto de prácticas engañosas como emisión falsa, manipulación de precios, operaciones entre cuentas relacionadas y promoción basada en expectativas irreales. La escasez aparente puede ser creada artificialmente mediante campañas, comunidades cerradas o compras coordinadas. Madanchian y Taherdoost (2024) explica que los modelos de negocio virtuales dependen de confianza, transparencia y

sostenibilidad. La ausencia de información sobre emisores, reservas, utilidad y condiciones de mercado incrementa el riesgo de pérdidas patrimoniales para los adquirentes.

La interoperabilidad de los NFT depende de que otras plataformas reconozcan el estándar, el archivo y la licencia. Un accesorio puede trasladarse técnicamente, pero no conservar su apariencia o funcionalidad en otro entorno. También puede ocurrir que la nueva plataforma rechace el contenido por incompatibilidad o por derechos de terceros. Kasiyanto y Kilinc (2022) señalan que la interoperabilidad requiere coordinación técnica y jurídica. La posibilidad de mover el token no garantiza que el activo mantenga idéntico valor, utilidad o reconocimiento.

La valoración económica de los NFT puede variar de manera intensa porque depende de factores especulativos, tecnológicos y comunitarios. El precio inicial no asegura una reventa futura ni refleja necesariamente el valor del contenido. Madanchian y Taherdoost (2024) sostiene que estos activos forman parte de modelos comerciales emergentes cuya sostenibilidad debe analizarse con cautela. Las plataformas y emisores deberían evitar mensajes que presenten aumentos de valor como resultados previsibles. El usuario necesita distinguir entre utilidad, colección, inversión y especulación antes de efectuar una adquisición.

3.5 Contratos electrónicos e inteligentes

Los contratos celebrados dentro del metaverso conservan naturaleza jurídica cuando existe una manifestación válida de voluntad y concurren los requisitos exigidos por el ordenamiento. La utilización de avatares, interfaces inmersivas, comandos de voz o sistemas automatizados no elimina la posibilidad de crear obligaciones. Sin embargo, la forma tecnológica puede dificultar que las partes comprendan cuándo una interacción constituye una simple acción dentro del entorno y cuándo produce consecuencias contractuales. La validez debe analizarse a partir del consentimiento, la capacidad, el objeto y la causa.

El Código Civil (2005), artículo 1454, define el contrato como el acto mediante el cual una parte se obliga frente a otra a dar, hacer o no hacer alguna cosa. Su artículo 1461 exige capacidad legal, consentimiento libre de vicios, objeto lícito y causa lícita. Estas condiciones también se aplican a operaciones virtuales. La existencia de una plataforma, un avatar o una cadena de bloques no sustituye los elementos jurídicos del

negocio. La tecnología modifica la forma de celebración o ejecución, pero no elimina los requisitos sustantivos.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002), artículo 44, reconoce efectos jurídicos a las transacciones realizadas mediante mensajes de datos. El artículo 45 impide negar validez o fuerza obligatoria a un contrato por haberse formado electrónicamente. Una compra, suscripción, prestación de servicios o transferencia realizada dentro del metaverso puede ser jurídicamente válida. La clave consiste en que la operación permita identificar la voluntad de las partes, su contenido y las obligaciones asumidas.

La manifestación del consentimiento puede expresarse mediante clics, gestos, comandos de voz, movimientos o selecciones dentro de una interfaz. Sin embargo, no toda acción debe interpretarse como aceptación contractual. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002), artículo 46, establece que la recepción, confirmación o apertura de un mensaje no implica necesariamente aceptación. En entornos inmersivos, la plataforma debe advertir claramente cuándo una conducta producirá un cobro, una transferencia o una obligación, evitando atribuir efectos jurídicos a movimientos ambiguos o cotidianos.

La información previa resulta esencial para que el consentimiento sea consciente. El usuario debe conocer el objeto, precio, duración, restricciones y consecuencias antes de confirmar la operación. Una interfaz visualmente atractiva no puede sustituir la explicación de los términos esenciales. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) exige comunicar condiciones y limitaciones de forma suficiente, mientras la legislación de consumo protege frente a información engañosa. El diseño debe permitir revisar la operación, corregir errores y cancelar antes de que la aceptación produzca efectos definitivos.

La capacidad también debe examinarse cuando intervienen menores, personas representadas o usuarios cuya identidad no ha sido verificada. La apariencia del avatar no permite determinar edad ni capacidad jurídica. Un personaje con aspecto adulto puede ser controlado por un menor y una representación infantil puede pertenecer a una persona mayor. Las operaciones de alto valor o riesgo requieren verificaciones proporcionales. La plataforma no debería basarse exclusivamente en rasgos visuales, sino en mecanismos adecuados que respeten simultáneamente privacidad y seguridad.

El error puede surgir por información incorrecta, fallos de interfaz, traducciones defectuosas o ejecución involuntaria de comandos. Una persona podría adquirir un objeto creyendo que se trata de una vista previa o aceptar un precio expresado de manera confusa. El Código Civil (2005) permite examinar los vicios del consentimiento, pero la arquitectura tecnológica influye en su aparición y prueba. El proveedor debe diseñar procedimientos que reduzcan errores previsibles y permitan confirmar operaciones antes de ejecutarlas, especialmente cuando existan transferencias irreversibles.

Los contratos de adhesión predominan en las relaciones entre plataformas y usuarios. Las condiciones suelen ser redactadas unilateralmente por el proveedor y aceptadas durante el registro. Esta estructura facilita el acceso, pero puede contener cláusulas que permitan modificar funciones, precios o activos sin suficiente justificación. La Ley Orgánica de Defensa del Consumidor (2000), artículo 43, declara nulas determinadas estipulaciones que limiten derechos, excluyan responsabilidad o coloquen al consumidor en indefensión. La aceptación electrónica no legitima cláusulas abusivas.

Los contratos inteligentes son programas que ejecutan automáticamente instrucciones cuando se cumplen condiciones predeterminadas. Pueden transferir tokens, distribuir pagos, liberar accesos o calcular regalías. Su denominación puede resultar engañosa, porque el código no siempre constituye por sí mismo un contrato completo. En algunos casos representa únicamente una herramienta de ejecución de un acuerdo previo. La calificación depende de si expresa obligaciones, identifica partes y contiene elementos suficientes para producir efectos jurídicos conforme al ordenamiento aplicable.

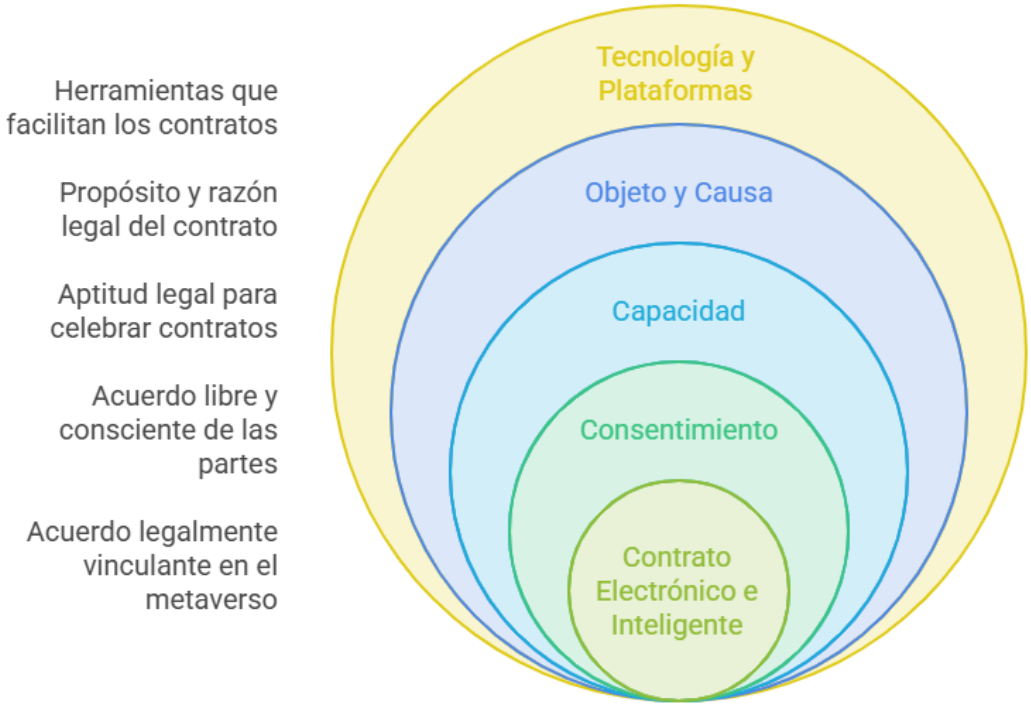
La automatización aporta rapidez y reduce determinadas intervenciones, pero también separa la ejecución del momento en que se verifica la validez jurídica. El programa puede transferir un activo, aunque la orden proceda de fraude, error o utilización ilegítima de credenciales. La exactitud informática del resultado no demuestra la legitimidad del negocio. Taherdoost (2023) identifica vulnerabilidades y errores de programación que justifican incorporar mecanismos de suspensión, revisión y restitución. La inmutabilidad del registro no puede prevalecer sobre la ausencia de consentimiento ni impedir el cumplimiento de una decisión judicial.

Cuando el resultado defectuoso se origina en el código, la atribución depende de reconstruir la intervención de quienes diseñaron, implementaron y administraron el sistema. El error puede proceder de una instrucción incorrecta, de información

suministrada por el usuario o de una vulnerabilidad explotada por terceros. Taherdoost (2023) sitúa la seguridad y el mantenimiento entre las limitaciones centrales de los contratos inteligentes. La responsabilidad no recae sobre el programa como si fuera un sujeto autónomo, sino sobre las personas u organizaciones cuya actuación, control o falta de diligencia contribuyó al resultado.

La confiabilidad del contrato inteligente también depende de las fuentes externas que comunican precios, fechas, resultados u otras condiciones al programa. Estos oráculos conectan el código con acontecimientos que no pueden verificarse directamente dentro de la cadena de bloques. Si la información es falsa, incompleta o manipulada, la ejecución puede resultar técnicamente coherente y jurídicamente incorrecta. Taherdoost (2023) advierte que la seguridad del sistema comprende tanto el código como las fuentes utilizadas. El acuerdo debe identificar al proveedor de información, los controles de verificación y el procedimiento aplicable frente a datos defectuosos.

Figura 8
Jerarquía de contratos electrónicos e inteligentes



Nota. La figura representa la relación jerárquica entre consentimiento, capacidad, objeto y causa, y tecnología en la formación de contratos electrónicos e inteligentes. Elaboración propia.

La prueba del contrato requiere conservar información sobre versión de términos, fecha, identidad, acción de aceptación y contenido de la operación. En una interfaz inmersiva, puede ser necesario registrar el comando, la confirmación y el resultado. Sin embargo, la conservación debe ser proporcional y no justificar vigilancia permanente. Los

registros deben demostrar la existencia del acuerdo sin almacenar todas las actividades del usuario. La autenticidad, integridad y trazabilidad serán esenciales cuando una parte desconozca la operación o alegue error, fraude o falta de consentimiento.

La modificación contractual exige especial cuidado cuando el usuario mantiene activos, saldos o actividades dependientes de la plataforma. Los cambios unilaterales pueden afectar valor, transferibilidad o acceso. El proveedor debe comunicar modificaciones relevantes con anticipación y permitir aceptar, rechazar o terminar la relación en condiciones razonables. Una cláusula general que autorice cualquier cambio no debería interpretarse como consentimiento ilimitado. La protección del consumidor exige previsibilidad y equilibrio frente al poder tecnológico y económico del operador.

La terminación del contrato puede producir consecuencias personales y patrimoniales. El cierre de una cuenta puede impedir acceder a obras, monedas, relaciones o servicios adquiridos. La plataforma debe establecer procedimientos claros sobre devolución de saldos, exportación de contenidos y destino de los activos. La terminación por incumplimiento también debe ser proporcional y ofrecer información suficiente. El contrato no puede convertir la suspensión en una pérdida automática e irreversible de todos los intereses acumulados cuando existan medidas menos gravosas.

Los contratos electrónicos e inteligentes del metaverso deben analizarse mediante los principios generales de contratación y las normas sobre comercio electrónico. La tecnología puede facilitar formación y ejecución, pero también introducir ambigüedad, automatización e irreversibilidad. La validez depende de consentimiento, capacidad, objeto y causa, mientras la ejecución requiere controles frente a error, fraude y fallos técnicos. Una regulación adecuada debe combinar seguridad tecnológica, transparencia contractual y mecanismos efectivos de corrección sin atribuir al código una autonomía jurídica que no posee.

3.6 Protección del consumidor virtual

La protección del consumidor virtual adquiere especial relevancia en el metaverso porque las decisiones económicas se desarrollan dentro de entornos inmersivos, interactivos y altamente personalizados. Los usuarios pueden adquirir objetos, servicios, entradas, monedas internas o activos digitales mediante interfaces que combinan imágenes, sonidos, recompensas y presión social. Estas características pueden dificultar una evaluación reflexiva de la operación. La protección jurídica debe

garantizar información suficiente, libertad de elección, seguridad en los pagos y mecanismos efectivos de reclamación frente a prácticas engañosas o prestaciones defectuosas.

La relación de consumo surge cuando una persona adquiere o utiliza bienes o servicios ofrecidos por un proveedor dentro del entorno virtual. La naturaleza digital del objeto no elimina la existencia de consumidor, proveedor, precio y obligación. Una plataforma puede vender directamente un activo, facilitar operaciones entre usuarios o permitir que terceros ofrezcan servicios. En cada caso debe identificarse quién formula la oferta, quién recibe el pago y quién responde por la prestación. La complejidad de la arquitectura no debe utilizarse para diluir la responsabilidad frente al consumidor.

La Ley Orgánica de Defensa del Consumidor (2000), artículo 4, reconoce el derecho a recibir información adecuada, veraz, clara, oportuna y completa. En el metaverso, esta obligación comprende precio, duración, funcionalidad, compatibilidad, transferibilidad y condiciones de pérdida o retiro. La información debe aparecer antes de la compra y no ocultarse en documentos extensos o menús secundarios. El consumidor necesita comprender si adquiere propiedad, licencia, suscripción o acceso temporal. La representación visual del objeto debe corresponder con las facultades realmente concedidas.

La identificación del proveedor constituye una condición básica de confianza. El usuario debe conocer el nombre o razón social, medios de contacto, jurisdicción y canales de reclamación. En mercados descentralizados o plataformas con múltiples vendedores, la interfaz debe diferenciar claramente al operador del proveedor directo. La falta de identidad verificable dificulta solicitar reembolso, exigir cumplimiento o iniciar acciones legales. La utilización de avatares o nombres comerciales no debe impedir conocer quién asume las obligaciones derivadas de la oferta y recibe los beneficios económicos.

El precio debe presentarse de manera comprensible. Las monedas internas, créditos y tokens pueden dificultar que el usuario identifique cuánto dinero real está utilizando. La plataforma debe mostrar la equivalencia en moneda de curso legal, las comisiones y cualquier costo adicional antes de confirmar la operación. También debe informar si el saldo puede expirar, perder valor o quedar bloqueado. La apariencia lúdica del sistema

no elimina la obligación de transparencia cuando la decisión produce una disminución patrimonial para el consumidor.

Los patrones oscuros son decisiones de diseño que orientan al usuario hacia opciones favorables para el proveedor mediante presión, confusión o dificultad artificial. Pueden manifestarse mediante botones de compra destacados, opciones de rechazo ocultas, conteos regresivos, escasez aparente o procesos complejos de cancelación. Munn y Weijers (2023) advierten que la arquitectura de los entornos virtuales puede condicionar la autonomía de los participantes. Estas prácticas deben evaluarse desde la transparencia, la lealtad comercial y la prohibición de inducir decisiones mediante mecanismos manipuladores.

Desde una perspectiva jurídica, los patrones oscuros no deben evaluarse únicamente como defectos visuales de la interfaz, sino como mecanismos capaces de afectar la autonomía decisoria del consumidor. Brenncke (2024) sostiene que estas prácticas pueden explotar sesgos conductuales mediante ocultamiento de información, obstáculos para cancelar, opciones preseleccionadas, presión repetitiva o presentación fragmentada del precio. La ilicitud debe determinarse considerando si el diseño reduce materialmente la capacidad de comprender, comparar o rechazar la operación. En el metaverso, esta evaluación debe incluir la arquitectura completa de la experiencia y no solamente el texto contractual mostrado al usuario.

La intensidad de este riesgo aumenta en entornos inmersivos, donde los estímulos visuales, espaciales, auditivos y hápticos pueden dirigir simultáneamente la atención y el movimiento. Wang et al. (2024) comprobaron que determinados diseños manipulativos en realidad aumentada pueden influir en las decisiones y acciones físicas de los participantes, incluso mediante recursos que atraen forzosamente su atención. Una interfaz inmersiva debería considerarse abusiva cuando utiliza proximidad, urgencia, estímulos corporales, obstáculos espaciales o recompensas para dificultar el rechazo o impulsar una compra que el consumidor no habría realizado en condiciones neutrales.

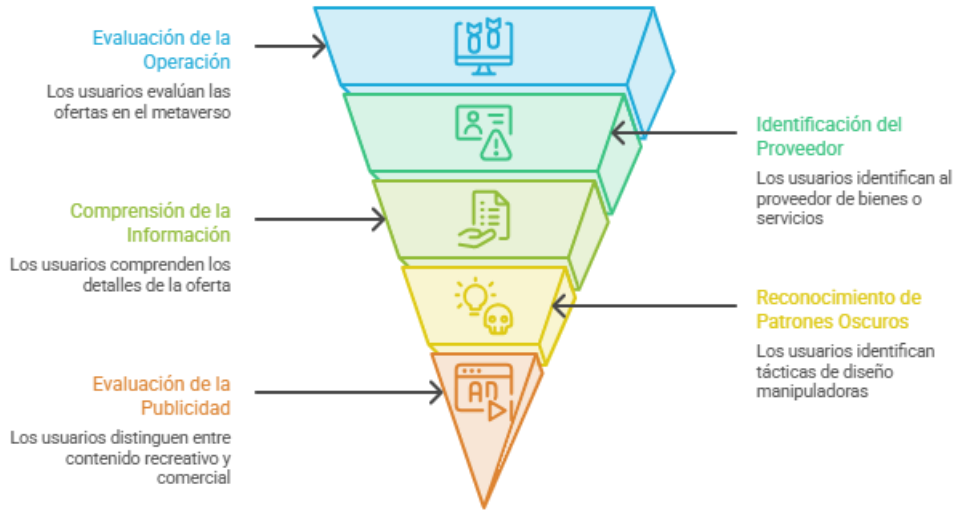
La publicidad dentro del metaverso puede incorporarse en escenarios, avatares, eventos, objetos o recomendaciones automáticas. Esta integración puede dificultar que el usuario distinga entre contenido recreativo y comunicación comercial. Toda promoción debe identificarse claramente, especialmente cuando intervienen personas influyentes,

personajes virtuales o agentes automatizados. El consumidor necesita saber cuándo una recomendación responde a un pago o interés económico. La publicidad encubierta impide valorar adecuadamente la finalidad del mensaje y puede aprovechar la confianza generada por la interacción inmersiva.

La personalización comercial utiliza información sobre recorridos, compras, contactos, tiempo de permanencia y reacciones del usuario. Esta práctica puede mejorar la relevancia de las ofertas, pero también facilitar manipulación, discriminación o precios diferenciados. La LOPDP (2021) exige que el tratamiento respete transparencia, finalidad, proporcionalidad y lealtad. Cuando la personalización depende de perfiles conductuales o inferencias emocionales, el consumidor debe conocer esa circunstancia y disponer de mecanismos para limitarla. La mejora del servicio no justifica una observación ilimitada de la conducta.

Las decisiones automatizadas pueden determinar qué productos se muestran, qué descuentos se ofrecen o qué consumidores reciben condiciones diferentes. Estas prácticas pueden producir discriminación económica si se basan en ubicación, comportamiento, nivel de gasto o inferencias sobre vulnerabilidad. La LOPDP (2021), artículo 20, resulta pertinente cuando la valoración automatizada genera efectos significativos. El usuario debe recibir información comprensible sobre los factores relevantes y contar con mecanismos de revisión. La personalización no debe convertirse en una forma oculta de exclusión o explotación.

Figura 9
Proceso de protección del consumidor en el metaverso



Nota. La figura presenta las etapas para proteger al consumidor en el metaverso mediante la evaluación

de la operación, la identificación del proveedor, la comprensión de la información y el reconocimiento de prácticas manipuladoras. Elaboración propia.

La calidad del bien o servicio también debe poder evaluarse. Un objeto virtual puede presentar fallos, incompatibilidad o pérdida de funcionalidad después de una actualización. Un evento puede cancelarse, tener interrupciones o no corresponder con lo anunciado. La Ley Orgánica de Defensa del Consumidor (2000) reconoce derechos relacionados con calidad, reparación y compensación. El proveedor debe ofrecer soluciones proporcionales, como corrección, sustitución, reembolso o crédito. La naturaleza intangible del bien no impide que exista incumplimiento cuando la prestación no satisface las condiciones ofrecidas.

Las cláusulas contractuales no deben permitir que la plataforma modifique unilateralmente elementos esenciales de la compra. La Ley Orgánica de Defensa del Consumidor (2000), artículo 43, declara nulas determinadas estipulaciones que limiten responsabilidad, impliquen renuncia de derechos o generen indefensión. Una cláusula que autorice retirar cualquier activo sin causa, cambiar retroactivamente su utilidad o retener saldos puede resultar abusiva. Las modificaciones relevantes deben comunicarse con anticipación y ofrecer al consumidor una opción razonable de aceptación, terminación o compensación.

El derecho de desistimiento o cancelación requiere adaptación a los servicios virtuales. Algunas prestaciones se ejecutan inmediatamente, mientras otras corresponden a suscripciones, eventos futuros o contenidos continuados. La plataforma debe explicar cuándo puede solicitarse devolución, qué condiciones se aplican y cómo cancelar. El procedimiento no debería ser más complejo que el utilizado para contratar. Los obstáculos deliberados, formularios innecesarios o recorridos confusos reducen la libertad del consumidor y pueden prolongar pagos que ya no desea mantener.

La protección de menores exige medidas reforzadas debido a su menor capacidad para comprender precios, publicidad y consecuencias patrimoniales. Las monedas internas, recompensas aleatorias y objetos de estatus pueden fomentar compras impulsivas. Los sistemas deben incorporar límites de gasto, confirmaciones adicionales, información apropiada para la edad y controles de representación. La autorización familiar no legitima diseños manipuladores ni publicidad invasiva. El interés superior exige que el modelo económico no dependa de explotar inexperiencia, presión social o dificultad para valorar el costo real.

Los mecanismos de reclamación deben ser accesibles dentro y fuera de la plataforma. El usuario necesita reportar cargos no reconocidos, fallos, incumplimientos o publicidad engañosa sin completar procedimientos desproporcionados. La respuesta debe indicar plazos, responsable y medidas adoptadas. Cuando la controversia involucra a un tercero vendedor, la plataforma debe explicar qué intervención ofrece y qué información conserva. La existencia de mercados abiertos no elimina la obligación de proporcionar vías claras para localizar al proveedor y gestionar conflictos.

La conservación de evidencia de una operación debe ser suficiente para demostrar oferta, aceptación, precio y prestación. Los recibos, historiales y términos aplicables deben permanecer accesibles en un formato comprensible. Sin embargo, esta finalidad no autoriza registrar de forma permanente toda la actividad del usuario. La documentación debe limitarse a la transacción y protegerse frente a alteraciones. Cuando exista un reclamo, el consumidor debe poder obtener una copia de la información relevante sin depender exclusivamente de capturas realizadas durante la experiencia.

En definitiva, la protección del consumidor virtual exige adaptar principios tradicionales a interfaces inmersivas, monedas internas y sistemas personalizados. La tecnología no reduce las obligaciones de información, calidad, seguridad y reparación. Por el contrario, el mayor poder de diseño de las plataformas requiere controles reforzados frente a patrones oscuros, publicidad encubierta y perfilamiento invasivo. Un mercado virtual jurídicamente sostenible debe permitir decisiones conscientes, identificar responsables y ofrecer mecanismos efectivos de reclamación, cancelación y restitución cuando la prestación no corresponda con lo ofrecido.

3.7 Propiedad intelectual digital

La propiedad intelectual digital adquiere especial importancia en el metaverso porque gran parte de su contenido es creado, modificado y comercializado por usuarios, desarrolladores y sistemas automatizados. Dentro de estos entornos pueden producirse imágenes, música, modelos tridimensionales, programas, diseños, escenarios, avatares y experiencias interactivas. La naturaleza digital de estas obras no elimina la protección jurídica. El análisis debe identificar quién creó el contenido, qué derechos conserva, qué licencias fueron concedidas y qué usos realiza la plataforma sobre los materiales incorporados al entorno (Al-Busaidi et al., 2024).

La creación realizada por los usuarios constituye uno de los principales motores de expansión de los mundos virtuales. Una persona puede diseñar una prenda, construir un espacio, producir una obra audiovisual o desarrollar una experiencia para otros participantes. Esta intervención puede generar derechos de autor cuando la creación posee originalidad y refleja decisiones creativas. La plataforma no se convierte automáticamente en titular por alojar, mostrar o comercializar el contenido. Las condiciones de servicio deben explicar con precisión si el usuario conserva sus derechos o concede una licencia de utilización.

La autoría debe diferenciarse de la titularidad patrimonial. El autor es quien realiza la creación intelectual, mientras los derechos económicos pueden ser transferidos, licenciados o gestionados por otras personas. En el metaverso, una obra puede ser creada por un usuario, comercializada por una plataforma y adquirida por un tercero. Cada intervención genera facultades distintas. Al-Busaidi et al. (2024) destacan que la adquisición de un activo digital no implica necesariamente la transmisión de los derechos sobre la obra incorporada, salvo que exista una autorización expresa.

Los derechos morales protegen la relación personal entre el autor y su creación. Comprenden, entre otras facultades, el reconocimiento de la autoría y la protección frente a modificaciones que afecten la integridad de la obra. Estas garantías pueden resultar relevantes cuando una plataforma altera un diseño, elimina la identificación del creador o incorpora la obra en contextos no autorizados. La facilidad técnica para transformar contenidos no elimina los derechos del autor. Debe distinguirse entre adaptación permitida, modificación contractual y alteración contraria a las condiciones de la licencia.

Los derechos patrimoniales permiten autorizar o prohibir reproducción, distribución, comunicación pública, transformación y explotación económica. En un mundo virtual, estos actos pueden ejecutarse mediante copias, exhibiciones, transmisiones, personalización de objetos o inclusión de una obra en experiencias comerciales. La compra de un archivo o token no concede automáticamente todas estas facultades. El usuario debe conocer si puede utilizar el contenido únicamente para fines personales, incorporarlo a otra creación o comercializarlo fuera de la plataforma (Martínez et al., 2024).

La licencia constituye el instrumento principal para ordenar el uso de obras digitales. Puede autorizar funciones específicas, limitar territorios, establecer plazos o permitir usos comerciales. En entornos virtuales, las licencias suelen incorporarse dentro de términos extensos que el usuario acepta durante el registro. Esta práctica puede dificultar la comprensión de las facultades concedidas. Kostenko et al. (2022) señalan que las plataformas deben diferenciar claramente entre derechos sobre el contenido creado, permisos de alojamiento y autorizaciones para promocionar, modificar o explotar económicamente la obra.

Al-Busaidi et al. (2024) advierten que la expansión de la inteligencia artificial y de la reutilización automatizada exige definir con precisión las licencias. La plataforma puede necesitar una licencia para almacenar, reproducir y mostrar los contenidos generados por los usuarios. Sin embargo, esa autorización debe ser proporcional a la prestación del servicio. Una cláusula que permita utilizar indefinidamente una obra para cualquier finalidad, incluso después del cierre de la cuenta, podría exceder lo necesario. La aceptación de términos generales no debería convertirse en una transferencia total y gratuita. El creador debe conocer el alcance, duración, sublicencias y posibles usos comerciales que realizará el operador.

La creación colaborativa plantea dificultades adicionales porque varias personas pueden intervenir sobre un mismo objeto o espacio. Un usuario puede diseñar la estructura, otro aportar imágenes y un tercero incorporar música o programación. La titularidad dependerá de la naturaleza de las contribuciones y de los acuerdos existentes. La plataforma debería facilitar mecanismos para identificar autores, registrar versiones y definir porcentajes de explotación. Sin esta información, pueden surgir controversias sobre reconocimiento, ingresos y autorización para modificar o retirar el contenido.

Los NFT requieren una separación precisa entre token, archivo, obra y licencia. El adquirente puede controlar el token sin adquirir derechos para reproducir o explotar el contenido. Martínez et al. (2024) sostienen que esta distinción es indispensable para evitar interpretaciones erróneas sobre propiedad intelectual. El emisor debe indicar si la operación incluye una licencia personal, comercial o ninguna autorización adicional. La transferencia del token no debería presentarse como cesión completa cuando el creador conserva los derechos patrimoniales y morales sobre la obra vinculada.

La reproducción no autorizada puede producirse mediante copias de objetos, capturas, descargas, extracción de modelos o replicación de avatares. La facilidad tecnológica amplía la circulación de contenidos, pero no elimina las restricciones jurídicas. Un objeto visible dentro de una plataforma no se convierte por ello en material de libre utilización. El contexto de acceso, la licencia y la finalidad del uso deben analizarse antes de copiar o incorporar una creación en otro entorno. La interoperabilidad puede aumentar estos riesgos al facilitar el traslado entre sistemas.

La utilización de marcas, logotipos y signos distintivos también puede generar conflictos. Los usuarios pueden reproducir nombres comerciales, uniformes, productos o establecimientos dentro de espacios virtuales. Algunos usos pueden responder a creación artística, crítica o representación ficticia, mientras otros buscan generar confusión o aprovechar reputación ajena. La valoración debe considerar finalidad, contexto y posibilidad de asociación con el titular. La plataforma necesita canales para denunciar imitaciones engañosas sin retirar automáticamente todo contenido que mencione o represente una marca.

La inteligencia artificial generativa introduce interrogantes sobre autoría, originalidad y utilización de contenidos preexistentes. Al-Busaidi et al. (2024) sostienen que los sistemas generativos pueden reproducir o transformar materiales protegidos y que los marcos tradicionales, centrados en la creación humana, no resuelven adecuadamente el entrenamiento, la opacidad de las plataformas ni la atribución de resultados. En el metaverso, estas dificultades se proyectan sobre imágenes, música, voces, escenarios y objetos tridimensionales, por lo que deben documentarse la intervención humana, las licencias y la procedencia de los materiales utilizados.

La determinación de autoría exige valorar la contribución humana concreta en la selección, dirección, corrección y configuración del resultado. Una instrucción genérica puede ser insuficiente para atribuir originalidad, mientras un proceso creativo documentado puede revelar decisiones intelectuales relevantes. Al-Busaidi et al. (2024) proponen examinar estas cuestiones mediante un enfoque dinámico que considere creación, reutilización, transparencia y equilibrio entre innovación y derechos de los titulares. La plataforma debe conservar información suficiente sobre el proceso sin convertir la trazabilidad en vigilancia permanente.

Al-Busaidi et al. (2024) identifican tensiones sobre entrenamiento, reutilización y explotación de contenidos protegidos. La apropiación indebida de contenidos puede ocurrir cuando la plataforma utiliza obras de usuarios para publicidad, entrenamiento algorítmico o creación de productos derivados sin autorización suficiente. Estas finalidades deben diferenciarse del almacenamiento necesario para prestar el servicio. La licencia debería explicar si el contenido se empleará para mejorar modelos, promocionar la plataforma o generar nuevas experiencias. La aceptación general no debe interpretarse como permiso ilimitado. El creador necesita mecanismos para oponerse, retirar contenido y reclamar cuando el uso exceda lo autorizado.

La retirada de una obra también plantea tensiones entre derechos del autor, compradores y continuidad del entorno. Un creador puede solicitar eliminar un contenido, pero terceros podrían haber adquirido licencias o incorporado el objeto en otras experiencias. La solución requiere examinar contratos, duración de autorizaciones y derechos previamente concedidos. La plataforma debe prever procedimientos para retirar la obra original sin destruir automáticamente todos los intereses legítimos derivados. También debe diferenciar entre eliminación visible, conservación restringida y preservación de evidencia frente a una controversia.

La prueba de autoría puede apoyarse en archivos originales, fechas de creación, historiales de versiones, registros de carga y sistemas distribuidos. Sin embargo, un registro técnico no demuestra por sí solo que la persona sea autora legítima. Puede existir apropiación previa, carga no autorizada o uso de contenido ajeno. La valoración debe considerar el proceso creativo, las fuentes utilizadas y la coherencia de los registros. La tecnología facilita trazabilidad, pero no sustituye la comprobación jurídica de originalidad, titularidad y autorización.

La propiedad intelectual digital exige distinguir entre creación, soporte, licencia, token y derechos asociados. El metaverso amplía las posibilidades de producción colaborativa y comercialización, pero también facilita copia, modificación y reutilización fuera del contexto original. La protección debe combinar reconocimiento de autoría, licencias claras, mecanismos de denuncia y transparencia sobre usos de la plataforma. Este apartado concentra el análisis de propiedad intelectual para evitar repetir posteriormente que la adquisición de un activo no transmite por sí sola todos los derechos sobre la obra incorporada (Martínez et al., 2024).

3.8 Tributación de operaciones virtuales

Las operaciones económicas desarrolladas en el metaverso pueden generar obligaciones tributarias cuando producen ingresos, ganancias, transferencias patrimoniales o prestaciones valorables. Lazea et al. (2025) muestran que la tributación de criptoactivos se organiza alrededor de la clasificación del ingreso, la residencia, la información disponible y el cumplimiento, con diferencias entre ganancias de capital, renta y actividad empresarial. La utilización de tokens, monedas internas o registros distribuidos no elimina el deber de identificar al contribuyente, valorar la operación y determinar el momento en que se realiza el hecho económico.

El principio de realidad económica resulta relevante para determinar la obligación tributaria. Una operación no deja de constituir una venta, prestación o ingreso por realizarse mediante avatares, contratos inteligentes o monedas virtuales. Debe examinarse qué recibió cada parte, cuál fue el valor de la contraprestación y si existió un incremento patrimonial. La denominación de recompensa, crédito, token o activo no sustituye el análisis de su función. La tributación debe concentrarse en los efectos económicos verificables y en la capacidad contributiva manifestada por la persona o empresa participante.

La identificación del contribuyente constituye uno de los principales desafíos. Los usuarios pueden actuar mediante seudónimos, cuentas descentralizadas o direcciones criptográficas que no revelan directamente su identidad civil. Sin embargo, las plataformas suelen conservar correos, medios de pago, historiales y dispositivos capaces de relacionar la actividad con una persona. Kasiyanto y Kilinc (2022) advierten que la descentralización dificulta localizar a los participantes, pero no elimina la existencia de responsables. Los mecanismos de identificación fiscal deben ser proporcionales y evitar una vigilancia indiscriminada.

La residencia fiscal continúa siendo un criterio central para determinar qué Estado puede gravar determinados ingresos. Un creador domiciliado en Ecuador puede recibir pagos de usuarios extranjeros mediante una plataforma administrada en otro país. La ubicación del servidor o de la cadena de bloques no define por sí sola la jurisdicción tributaria. Deben considerarse residencia del contribuyente, lugar de desarrollo de la actividad, fuente del ingreso y establecimiento del proveedor. La naturaleza

transfronteriza exige coordinación para reducir vacíos, doble imposición y dificultades de fiscalización.

La valoración de los activos digitales constituye otro problema importante. El precio de un NFT, terreno virtual o token puede expresarse en criptomonedas, monedas internas o bienes intercambiados. Para efectos tributarios, debe determinarse su valor en moneda de curso legal al momento relevante. La volatilidad puede producir diferencias significativas entre adquisición, transferencia y conversión. Lazea et al. (2025) muestran que el token, el archivo y los derechos asociados son elementos distintos, por lo que la valoración debe identificar exactamente qué activo o facultad fue objeto de la operación.

Las monedas internas requieren una evaluación diferenciada. Algunas solo permiten adquirir servicios dentro de una plataforma y no pueden convertirse en dinero oficial, mientras otras son transferibles o canjeables. La existencia de un saldo virtual no siempre representa inmediatamente un ingreso disponible. Debe analizarse cuándo el usuario obtiene control económico, si puede retirar los fondos y si existe una contraprestación por una actividad realizada. La tributación no debería adelantarse a valores puramente ficticios, pero tampoco ignorar recursos que pueden transformarse en beneficios patrimoniales reales.

Tabla 9
Tratamiento tributario preliminar de operaciones realizadas en el metaverso

Operación virtual	Posible naturaleza económica	Elemento que debe identificarse	Riesgo tributario
Venta de accesorio digital	Ingreso por actividad comercial	Precio y titular de la venta	Omisión de ingresos
Prestación de servicio mediante avatar	Honorario o ingreso profesional	Lugar y beneficiario del servicio	Dificultad para localizar la fuente
Transferencia de NFT	Venta o ganancia patrimonial	Costo, precio y derechos transferidos	Valoración incorrecta
Regalía automática	Rendimiento por licencia	Autor, contrato y periodicidad	Falta de declaración
Alquiler de espacio virtual	Ingreso por cesión temporal	Duración y contraprestación	Confusión con compraventa
Recompensa por creación	Remuneración por actividad	Causa económica del pago	Clasificación inadecuada

Operación virtual	Posible naturaleza económica	Elemento que debe identificarse	Riesgo tributario
Conversión de moneda interna	Realización de valor virtual	Tipo de cambio y fecha	Subvaloración
Publicidad inmersiva	Ingreso empresarial o profesional	Anunciante y plataforma	Pagos transfronterizos opacos
Comisión de plataforma	Ingreso por intermediación	Porcentaje y volumen de operaciones	Falta de trazabilidad
Donación de activo digital	Transferencia gratuita	Valor y relación entre las partes	Ocultamiento de contraprestaciones

Nota. La calificación definitiva depende de la legislación tributaria, la residencia del contribuyente y las características económicas comprobables de cada operación.

Lazea et al. (2025) muestran que la investigación tributaria sobre criptoactivos se concentra crecientemente en calificación, cumplimiento y trazabilidad. La venta de contenidos creados por usuarios puede constituir una actividad habitual o una operación ocasional. Esta diferencia influye en la forma de registrar ingresos, costos y obligaciones. Un diseñador que comercializa sistemáticamente objetos virtuales presenta una situación distinta de quien transfiere una única creación. Deben considerarse frecuencia, organización, intención económica y continuidad. La plataforma puede aportar información sobre ventas, comisiones y retiros, pero la automatización del mercado no sustituye la obligación del contribuyente de documentar adecuadamente sus actividades.

Las regalías programadas mediante contratos inteligentes también pueden generar ingresos tributables. Un creador puede recibir automáticamente un porcentaje cada vez que su activo se revende. La distribución se ejecuta sin intervención manual, pero conserva una causa económica vinculada con la explotación de una creación o licencia. Ness (2024) destaca la importancia de diferenciar el token del contenido o derecho subyacente al analizar el tratamiento fiscal de estas operaciones. La automatización del pago no elimina la obligación de identificar su naturaleza económica.

Lazea et al. (2025) identifican la valoración y determinación de ganancias como ejes recurrentes de la fiscalidad de criptoactivos. Las ganancias derivadas de la transferencia de activos digitales requieren establecer costo de adquisición y valor de enajenación. Esta determinación puede resultar difícil cuando el activo fue obtenido mediante intercambio, recompensa, creación propia o pago en criptomonedas. También deben considerarse comisiones y gastos directamente relacionados. La ausencia de

comprobantes tradicionales no impide reconstruir la operación mediante registros de plataforma, contratos y transacciones distribuidas. Sin embargo, la trazabilidad técnica debe vincularse con la identidad y con la naturaleza económica real del negocio.

La tributación indirecta también puede intervenir cuando se prestan servicios o se comercializan bienes digitales. Ness (2024) evidencia que la aplicación del IVA o GST a bitcoin y NFT presenta problemas de clasificación, neutralidad y armonización, especialmente cuando no se distingue entre medio de pago, activo y servicio asociado. En el metaverso deben examinarse el lugar de consumo, la condición del proveedor, la naturaleza del derecho adquirido y la intervención de plataformas intermediarias, evitando aplicar una misma categoría fiscal a operaciones económicamente diferentes.

Ness (2024) evidencia que la calificación tributaria de activos y servicios digitales condiciona la determinación de la base imponible. Los costos y gastos vinculados con actividades virtuales pueden incluir desarrollo, dispositivos, comisiones, almacenamiento, publicidad y adquisición de licencias. Su deducibilidad dependerá de que se relacionen con la generación de ingresos, se encuentren respaldados y cumplan las condiciones legales. Un creador profesional podría justificar gastos distintos de los correspondientes a un consumidor ocasional. La mezcla entre uso personal y actividad económica exige separación razonable. Los registros digitales deben conservar información suficiente para demostrar la relación entre el gasto, la operación y el ingreso declarado.

La trazabilidad de las cadenas de bloques puede facilitar el seguimiento de operaciones, pero no resuelve todos los problemas fiscales. Los registros muestran direcciones, fechas y montos, aunque no necesariamente revelan identidad, residencia o causa jurídica. Una transferencia puede corresponder a venta, donación, devolución o movimiento entre cuentas del mismo titular. Kasiyanto y Kilinc (2022) señalan que la información técnica debe interpretarse dentro del contexto jurídico y económico. La administración tributaria necesita combinar análisis tecnológico, documentación y garantías para evitar conclusiones automáticas.

Ness (2024) destaca que la intermediación digital puede influir en identificación, documentación y cumplimiento tributario. Las plataformas pueden desempeñar una función importante en la generación de información tributaria. Conocen operaciones, comisiones, saldos y mecanismos de retiro, por lo que podrían emitir reportes accesibles

para usuarios y autoridades competentes. Sin embargo, esta colaboración debe respetar la protección de datos y limitarse a información pertinente. La fiscalización no justifica recopilar conversaciones, movimientos corporales o relaciones sociales. El deber de informar debe concentrarse en transacciones económicas, identidad fiscal cuando corresponda y datos necesarios para verificar obligaciones legalmente establecidas.

Lazea et al. (2025) muestran que la cooperación y el intercambio de información constituyen tendencias centrales de la tributación de criptoactivos. La cooperación internacional resulta indispensable cuando intervienen plataformas, compradores y vendedores situados en distintos países. Sin intercambio de información, pueden producirse vacíos de tributación o imposición duplicada. Los criterios deben coordinar residencia, fuente y lugar de consumo. También se requieren mecanismos para identificar establecimientos digitales y actividades dirigidas de manera sostenida al mercado ecuatoriano. La solución no consiste en considerar que toda interacción global genera obligación en todos los países, sino en establecer conexiones económicas suficientemente claras, previsibles y verificables.

La ausencia de reglas detalladas puede generar inseguridad tanto para contribuyentes como para la administración. Una persona podría desconocer cuándo una recompensa virtual constituye ingreso o cómo valorar un activo recibido. Al mismo tiempo, interpretaciones excesivamente amplias podrían gravar valores que no son utilizables ni convertibles. La regulación debe diferenciar adquisición, tenencia, intercambio, venta y conversión. También debe establecer criterios para pérdidas, activos sin liquidez y operaciones anuladas. La claridad normativa reduce evasión, errores involuntarios y tratamientos inconsistentes entre actividades económicamente semejantes.

Por lo cual se comprende que la tributación de operaciones virtuales debe basarse en la realidad económica, la residencia, la fuente del ingreso y la capacidad contributiva. El metaverso modifica la forma de producir y transferir valor, pero no elimina las obligaciones fiscales derivadas de ingresos y ganancias. Los principales desafíos se relacionan con identidad, valoración, localización y trazabilidad. Una respuesta adecuada requiere reglas comprensibles, cooperación internacional y protección proporcional de datos, evitando tanto la ausencia de control como la fiscalización indiscriminada de toda actividad desarrollada dentro de los mundos virtuales.

Capítulo 4

Responsabilidad jurídica y delitos en entornos virtuales

Karla Daniela Argoti Trujillo



4.1 Responsabilidad jurídica en el metaverso

La responsabilidad jurídica en el metaverso surge cuando una conducta, decisión tecnológica u omisión produce un daño, incumplimiento o afectación jurídicamente relevante. Su análisis no depende exclusivamente del medio virtual utilizado, sino de la relación entre el hecho, los actores involucrados y las consecuencias generadas. Los mundos inmersivos pueden reunir usuarios, plataformas, desarrolladores, fabricantes y sistemas automatizados dentro de una misma experiencia. Atribuir responsabilidad exige identificar quién controlaba la actividad, qué obligación debía cumplir y qué medidas podía adoptar para prevenir el resultado (Kasiyanto y Kilinc, 2022).

La representación mediante avatares no crea sujetos jurídicos autónomos. Las acciones ejecutadas dentro del entorno deben atribuirse a personas naturales o jurídicas, aunque la identificación pueda ser compleja por el uso de seudónimos, credenciales compartidas o sistemas automatizados. La titularidad formal de una cuenta constituye un indicio, pero no demuestra por sí sola quién realizó la conducta. Una atribución adecuada requiere considerar registros de acceso, mecanismos de autenticación, dispositivos utilizados y circunstancias contextuales que permitan vincular razonablemente el acto con su responsable (Pooyandeh et al., 2022).

La responsabilidad puede ser contractual cuando el daño deriva del incumplimiento de obligaciones aceptadas entre usuarios, proveedores o plataformas. Una empresa puede comprometerse a prestar acceso, conservar determinados contenidos, ejecutar una transacción o proteger una cuenta. Si la prestación no se cumple conforme a lo ofrecido, pueden surgir deberes de reparación. El Código Civil (2005) permite examinar incumplimiento, mora, daño emergente y lucro cesante. La virtualidad modifica la forma de prestación, pero no elimina la obligación de cumplir aquello que fue jurídicamente acordado.

La responsabilidad extracontractual aparece cuando una conducta causa daño sin que exista necesariamente una relación contractual previa entre responsable y afectado. Puede presentarse mediante agresiones virtuales, difusión de información, destrucción de activos, uso no autorizado de identidades o fallos tecnológicos. El Código Civil (2005), artículo 2214, establece la obligación de indemnizar cuando un delito o cuasidelito ocasiona daño. La aplicación de esta norma exige comprobar conducta, afectación, relación causal y un criterio de imputación atribuible al responsable.

El daño constituye un elemento indispensable de la responsabilidad civil. No toda incomodidad, conflicto o experiencia negativa dentro del metaverso genera automáticamente una obligación de reparar. Debe existir una afectación verificable sobre intereses personales, patrimoniales, reputacionales o psicológicos. Munn y Weijers (2023) sostienen que la intensidad de la presencia virtual puede aumentar el impacto de ciertas interacciones. Sin embargo, la valoración debe considerar duración, reiteración, contexto, vulnerabilidad del afectado y consecuencias producidas dentro y fuera del entorno digital.

La causalidad puede ser difícil de establecer cuando intervienen múltiples componentes tecnológicos. Un daño puede derivar de la conducta de un usuario, un error de software, una falla del dispositivo o una decisión de la plataforma. También pueden concurrir varios factores. La investigación debe determinar si el resultado era consecuencia razonablemente vinculada con la conducta analizada. No basta afirmar que el daño ocurrió dentro de una plataforma determinada. Debe demostrarse cómo cada intervención contribuyó materialmente a producir o agravar la afectación.

La culpa puede manifestarse mediante imprudencia, negligencia, falta de previsión o incumplimiento de deberes de cuidado. Un usuario puede actuar negligentemente al compartir credenciales, mientras una plataforma puede omitir medidas básicas frente a riesgos conocidos. La valoración debe considerar el nivel de conocimiento, capacidad técnica y control de cada actor. No se exige la misma diligencia a un participante ocasional que a una empresa especializada que diseña la infraestructura y obtiene beneficios económicos de su funcionamiento.

La responsabilidad objetiva podría resultar aplicable en actividades de riesgo cuando la legislación lo permita y la naturaleza de la actividad justifique prescindir de la culpa como elemento central. Los dispositivos inmersivos, sistemas automatizados y operaciones de alto valor pueden generar riesgos difíciles de controlar para el usuario. Sin embargo, no debe presumirse responsabilidad objetiva para toda actividad virtual. Su utilización requiere fundamento jurídico, identificación del riesgo especial y relación entre la actividad y el daño producido, evitando convertir cualquier innovación tecnológica en fuente automática de indemnización.

Tabla 10
Elementos para determinar responsabilidad jurídica en el metaverso

Elemento	Pregunta principal	Evidencia relevante	Riesgo de valoración incorrecta
Conducta	¿Qué acción u omisión ocurrió?	Registros, mensajes y actividad de cuenta	Confundir fallo técnico con decisión humana
Autoría	¿Quién controlaba la cuenta o sistema?	Accesos, dispositivos y autenticación	Atribuir automáticamente al titular
Daño	¿Qué afectación verificable se produjo?	Pérdidas, informes y consecuencias	Considerar responsable toda experiencia negativa
Causalidad	¿La conducta produjo el resultado?	Secuencia temporal y análisis técnico	Ignorar factores concurrentes
Culpa	¿Existió negligencia o falta de cuidado?	Medidas adoptadas y riesgo conocido	Exigir igual diligencia a todos los actores
Control	¿Quién podía modificar o impedir la conducta?	Permisos, funciones y arquitectura	Responsabilizar a quien carecía de intervención
Previsibilidad	¿El daño podía anticiparse razonablemente?	Incidentes previos y advertencias	Imputar riesgos imprevisibles
Beneficio	¿Quién obtenía ventaja de la actividad?	Ingresos, comisiones y modelo económico	Separar beneficio de obligaciones
Prevención	¿Qué medidas razonables estaban disponibles?	Herramientas, políticas y protocolos	Exigir prevención absoluta
Reparación	¿Qué medida restablece mejor el derecho?	Recuperación, retiro o indemnización	Aplicar respuestas desproporcionadas

Nota. La responsabilidad debe establecerse mediante una valoración conjunta y no a partir de un solo elemento técnico o contractual.

La responsabilidad de los usuarios puede derivar de conductas como amenazas, acoso, fraude, apropiación de cuentas o uso no autorizado de contenidos. La utilización de un avatar no reduce la relevancia de la conducta cuando afecta a otra persona. Sin embargo, la imputación requiere verificar que el usuario controlaba efectivamente la representación y actuó con el grado de intención o negligencia exigido. González (2023) destaca que los comportamientos virtuales deben analizarse según sus efectos emocionales y jurídicos, evitando tanto minimizar como exagerar su gravedad.

Los desarrolladores pueden asumir responsabilidad cuando un defecto de diseño o programación produce daños previsibles. Esto puede ocurrir si una función permite accesos indebidos, ejecuta transferencias erróneas o expone datos sin medidas

adecuadas. La responsabilidad no surge por la simple existencia de un fallo, sino por la relación entre defecto, riesgo y daño. Debe analizarse si el problema era conocido, si podía corregirse y si el producto se ofreció sin advertencias suficientes. La complejidad técnica no elimina los deberes profesionales de diseño y prueba.

Los fabricantes de dispositivos inmersivos también pueden intervenir en la producción del daño. Un visor, sensor o dispositivo háptico defectuoso puede provocar lesiones, desorientación o respuestas físicas inadecuadas. La evaluación debe distinguir entre mal uso, falta de mantenimiento, error de software y defecto del producto. Cuando varios componentes funcionan conjuntamente, puede ser necesario distribuir responsabilidad entre fabricante, desarrollador y operador. La persona afectada no debería soportar la imposibilidad de identificar internamente qué proveedor controlaba cada parte del sistema.

La responsabilidad de las plataformas depende de su grado de intervención sobre la actividad. El operador administra cuentas, define reglas, organiza funciones y posee capacidad para modificar contenidos o suspender usuarios. No puede considerarse responsable automáticamente por todo acto de terceros, pero tampoco puede presentarse como neutral cuando controla aspectos esenciales del entorno. Kasiyanto y Kilinc (2022) señalan que la imputación debe atender al control efectivo, conocimiento del riesgo y capacidad de prevención. Este tema será desarrollado específicamente en el apartado 4.3.

Los sistemas de inteligencia artificial pueden intervenir en recomendaciones, moderación, generación de contenido y decisiones sobre acceso. Sin embargo, el sistema no posee personalidad jurídica ni responde por sí mismo. La responsabilidad debe dirigirse hacia quienes lo desarrollan, implementan, entrenan o utilizan. Debe analizarse si el daño derivó de datos defectuosos, diseño inadecuado, falta de supervisión o utilización incorrecta. La autonomía técnica puede aumentar la complejidad de la atribución, pero no elimina la necesidad de identificar decisiones humanas y organizacionales.

La concurrencia de responsabilidades puede presentarse cuando varios actores contribuyen al mismo resultado. Un usuario puede ejecutar una conducta dañina, mientras la plataforma omite responder a denuncias y el sistema automatizado amplifica el contenido. En estos casos, la distribución debe considerar el aporte causal, el control

y la capacidad de prevención de cada participante. No resulta adecuado atribuir toda la responsabilidad al actor más visible ni absolver a quienes facilitaron o prolongaron el daño mediante decisiones técnicas o empresariales.

La reparación debe adaptarse a la naturaleza de la afectación. Puede incluir indemnización, recuperación de cuentas, restitución de activos, retiro de contenido, rectificación de perfiles o corrección de decisiones automatizadas. En algunos casos, la reparación económica será insuficiente si continúa circulando una representación falsa o persiste una sanción basada en datos incorrectos. La respuesta debe procurar restablecer la situación del afectado y evitar la continuidad del daño, sin imponer medidas más gravosas de lo necesario para proteger el derecho comprometido.

La responsabilidad jurídica en el metaverso exige, en consecuencia, un análisis funcional de conducta, control, daño, causalidad y prevención. No debe atribuirse responsabilidad únicamente por la titularidad de una cuenta, la propiedad de una plataforma o la existencia de tecnología automatizada. Cada actor debe responder según su participación real y las obligaciones que podía cumplir. Este enfoque permite aplicar las categorías tradicionales de responsabilidad sin desconocer las particularidades de los entornos inmersivos ni utilizar fuentes sobre NFT o consentimiento para fundamentar cuestiones ajenas a su objeto.

4.2 Daños en entornos virtuales

Los daños producidos en entornos virtuales pueden afectar intereses personales, patrimoniales, reputacionales y psicológicos, aunque la conducta se ejecute mediante avatares o sistemas digitales. La ausencia de contacto físico directo no significa que la afectación carezca de relevancia jurídica. Amenazas, persecuciones, pérdida de activos, difusión de contenidos o alteración de identidades pueden generar consecuencias reales sobre la vida de los usuarios. El análisis debe considerar la naturaleza de la conducta, la intensidad de la experiencia, la duración del daño y sus efectos dentro y fuera de la plataforma (Munn y Weijers, 2023).

El daño patrimonial aparece cuando una conducta ocasiona pérdida de bienes, saldos, oportunidades económicas o ingresos. Puede producirse mediante apropiación de cuentas, transferencias fraudulentas, eliminación de activos o incumplimiento de servicios contratados. La valoración debe determinar el valor real del perjuicio y distinguir entre expectativas especulativas y pérdidas verificables. El precio pagado, la

utilidad del activo, su posibilidad de transferencia y la existencia de un mercado permiten aproximarse a la cuantificación. No todo descenso de valor genera responsabilidad, especialmente cuando deriva de riesgos previamente informados.

Los daños reputacionales pueden surgir cuando una persona es asociada con expresiones, conductas o contenidos que no realizó. La copia de un avatar, la difusión de mensajes falsos o la creación de perfiles engañosos puede afectar relaciones laborales, académicas o comerciales. Sorrentino y López (2025) explican que las representaciones virtuales pueden integrar elementos biométricos y conductuales suficientemente vinculados con una persona identificable. La reparación debe considerar retiro, rectificación y corrección de historiales cuando la información falsa continúa influyendo en decisiones posteriores.

Los daños a la intimidad pueden producirse mediante grabación, vigilancia, divulgación o reutilización de información obtenida durante la experiencia virtual. Las plataformas pueden registrar voz, mirada, movimientos, conversaciones y características del entorno físico. Una filtración o uso secundario puede revelar hábitos, relaciones o condiciones que la persona no decidió comunicar. Sorrentino y López (2025) advierten que los datos inferidos aumentan la profundidad de la exposición. La afectación no depende únicamente de la publicación, pues también puede derivar del seguimiento oculto y del perfilamiento persistente.

Los daños psicológicos requieren una valoración cuidadosa porque la presencia virtual puede intensificar determinadas experiencias. Una persecución reiterada, una amenaza creíble o una interacción sexual no consentida puede provocar miedo, ansiedad, vergüenza o abandono de la plataforma. Munn y Weijers (2023) sostienen que la inmersión puede hacer que ciertos acontecimientos sean percibidos de manera especialmente cercana. Sin embargo, la existencia del daño debe evaluarse mediante consecuencias comprobables, contexto, reiteración y características personales, evitando presumir automáticamente una lesión psicológica ante cualquier interacción desagradable.

La violencia virtual puede adoptar formas verbales, visuales, espaciales o sensoriales. Puede expresarse mediante insultos, gestos intimidatorios, persecución del avatar, encierro en espacios, difusión de contenido degradante o activación de estímulos hápticos. Chawki et al. (2024) señala que los entornos virtuales pueden reproducir

formas de agresión que requieren respuestas jurídicas y tecnológicas coordinadas. La valoración debe considerar la finalidad, el control ejercido por el agresor, la posibilidad de abandonar la interacción y el impacto producido sobre la persona afectada.

Los daños derivados de interacciones sexuales no consentidas presentan especial complejidad. La aproximación de avatares, la simulación de contacto o la utilización de dispositivos hápticos puede generar una experiencia invasiva, aunque no exista contacto corporal físico entre las personas. González (2023) destaca que la relevancia penal y emocional de estas conductas depende del contexto, la intención y la afectación. El consentimiento para ingresar a un entorno no implica aceptar cualquier interacción. Los límites personales deben poder establecerse y modificarse durante la experiencia.

Los daños por discriminación pueden manifestarse mediante exclusión de espacios, restricciones de acceso, insultos o decisiones automatizadas basadas en rasgos reales o virtuales. La apariencia del avatar puede utilizarse para reproducir prejuicios relacionados con género, etnia, discapacidad, edad o expresión cultural. Jauhiainen et al. (2023) advierten que los mundos virtuales pueden reproducir desigualdades preexistentes. La existencia del daño debe analizarse según la conducta, la reiteración, el contexto y las consecuencias sobre la participación efectiva de la persona dentro de la comunidad.

Los daños tecnológicos pueden provenir de defectos de software, errores de sensores, fallos de conexión o funcionamiento inadecuado de dispositivos. Una descoordinación puede provocar pérdida de información, transferencias erróneas o lesiones físicas. La responsabilidad dependerá de si el defecto era previsible, si existían medidas de prevención y qué actor controlaba el componente afectado. Deben distinguirse los errores propios del usuario de las fallas atribuibles al fabricante, desarrollador o proveedor. La complejidad técnica no elimina la necesidad de identificar la causa concreta del daño.

Los daños continuados presentan especial gravedad porque el contenido o la clasificación perjudicial puede permanecer activa durante largos periodos. Una réplica, mensaje, sanción o perfil inexacto puede seguir produciendo consecuencias aunque la conducta inicial haya cesado. Chawki et al. (2024) destaca que la persistencia y replicabilidad de los entornos digitales amplifican determinadas afectaciones. La reparación debe orientarse no solo al hecho original, sino también a detener su

circulación, corregir bases de datos y evitar que sistemas automatizados continúen utilizando información perjudicial.

La prueba del daño puede apoyarse en registros de actividad, capturas, comunicaciones, informes técnicos, historiales de transacción y testimonios. En casos psicológicos o profesionales también pueden resultar relevantes informes especializados y evidencia sobre cambios en la conducta o pérdida de oportunidades. Sin embargo, la preservación debe respetar la intimidad de otras personas. No resulta adecuado registrar indiscriminadamente todas las interacciones. La información debe limitarse al incidente, conservarse de forma segura y permitir reconstruir de manera suficiente la secuencia de acontecimientos.

La valoración económica del daño virtual puede ser compleja cuando involucra activos sin mercado estable, reputación o afectaciones emocionales. El precio pagado no siempre coincide con el valor real, especialmente en activos especulativos. También puede existir lucro cesante cuando la pérdida de una cuenta impide continuar una actividad profesional. La cuantificación debe apoyarse en datos verificables, historial de ingresos, utilidad y alcance de la afectación. Las expectativas meramente hipotéticas no deben equipararse con ganancias ciertas que razonablemente habrían sido obtenidas.

La conducta de la víctima puede influir en la valoración cuando contribuye materialmente al resultado, pero no debe utilizarse para trasladarle toda la responsabilidad. Compartir una contraseña, ignorar advertencias o mantener configuraciones inseguras puede ser relevante para distribuir el daño. Sin embargo, el proveedor conserva sus propias obligaciones de seguridad y respuesta. La evaluación debe evitar argumentos que culpabilicen a la persona afectada por participar, confiar o utilizar funciones normales de la plataforma. La responsabilidad debe distribuirse según la intervención real de cada actor.

Las medidas preventivas son esenciales porque algunos daños resultan difíciles de revertir. Las plataformas pueden incorporar bloqueo, límites espaciales, alertas de acceso, confirmaciones de transacción y configuraciones de privacidad. Sakka et al. (2026) destacan que los límites digitales deben poder expresarse durante la experiencia. Estas herramientas no eliminan la responsabilidad cuando el daño ya se produjo, pero reducen riesgos previsibles y facilitan una respuesta inmediata. La prevención debe adaptarse al tipo de interacción y no depender únicamente de denuncias posteriores.

La reparación debe ser integral y proporcional. Puede incluir restitución de activos, recuperación de cuentas, retiro de contenido, rectificación, compensación económica y medidas para impedir nuevas afectaciones. En daños de identidad o reputación, la indemnización por sí sola puede resultar insuficiente si persiste el contenido falso. En daños psicológicos, puede requerirse apoyo especializado. La respuesta debe considerar la naturaleza, duración y alcance del perjuicio, evitando aplicar una solución uniforme a conductas y consecuencias diferentes.

Los daños en entornos virtuales no deben minimizarse por su origen digital ni equipararse automáticamente con daños físicos. Su valoración exige examinar experiencia, contexto, evidencia y efectos reales. Munn y Weijers (2023), Chawki et al. (2024) y González (2023) ofrecen fundamentos adecuados para comprender la intensidad y diversidad de estas afectaciones. El derecho debe responder de forma proporcional, diferenciando conflicto, molestia, riesgo y daño verificable, y reservando las fuentes sobre NFT o consentimiento para los supuestos en que sean verdaderamente pertinentes.

4.3 Responsabilidad de las plataformas

Las plataformas del metaverso cumplen una función central porque diseñan la arquitectura, administran cuentas, organizan interacciones y establecen las reglas de funcionamiento. Su responsabilidad jurídica no surge automáticamente por toda conducta ejecutada por los usuarios, pero tampoco puede descartarse cuando poseen capacidad efectiva para prevenir, limitar o corregir daños. La valoración debe considerar el grado de control sobre el entorno, el conocimiento del riesgo, la intervención realizada y las medidas disponibles. La estructura tecnológica y contractual determina qué deberes podían exigirse razonablemente al operador.

La posición de la plataforma debe analizarse según las funciones que realmente desempeña. Algunas se limitan a proporcionar infraestructura, mientras otras seleccionan contenidos, procesan pagos, administran activos, personalizan experiencias y aplican sanciones. Cuanto mayor sea la intervención sobre la actividad, más difícil resulta considerarla un intermediario completamente neutral. Kasiyanto y Kilinc (2022) señalan que la responsabilidad en entornos virtuales debe distribuirse según control, beneficio y capacidad de decisión, evitando categorías generales que desconozcan las diferencias entre modelos de administración.

El deber de diligencia exige identificar riesgos previsibles relacionados con seguridad, privacidad, fraude, acoso y funcionamiento de los servicios. La plataforma no está obligada a impedir absolutamente toda conducta dañina, pero debe adoptar medidas proporcionales al tamaño, finalidad y nivel de riesgo del entorno. Un espacio dirigido a menores o utilizado para operaciones económicas requiere controles más rigurosos que una comunidad pequeña y cerrada. La previsibilidad puede demostrarse mediante incidentes anteriores, denuncias, vulnerabilidades conocidas y advertencias emitidas por especialistas o autoridades.

La seguridad desde el diseño constituye una de las principales obligaciones técnicas. La plataforma debe incorporar autenticación, gestión de permisos, cifrado, actualizaciones y mecanismos de recuperación antes de que ocurra un incidente. Pooyandeh et al. (2022) destacan que los entornos virtuales amplían la superficie de ataque por la conexión entre cuentas, sensores, comunicaciones y activos. Estas medidas no fundamentan por sí solas toda responsabilidad jurídica del intermediario, pero permiten evaluar si el operador adoptó controles razonables frente a riesgos técnicos conocidos.

El diseño de las funciones también puede contribuir directamente a la producción del daño. Una plataforma que permite contactos invasivos, transferencias sin confirmación o acceso excesivo a sensores crea condiciones que aumentan determinados riesgos. En estos casos, la responsabilidad no se basa únicamente en la conducta de un tercero, sino en decisiones de arquitectura. Munn y Weijers (2023) advierten que el diseño distribuye poder y condiciona la autonomía de los participantes. Las medidas preventivas deben integrarse en las funciones normales y no depender exclusivamente de configuraciones difíciles de encontrar.

Los términos de servicio constituyen otro ámbito de responsabilidad. La plataforma puede definir reglas sobre contenidos, activos, sanciones y resolución de controversias, pero estas condiciones deben ser claras y compatibles con normas imperativas. No resulta admisible utilizar cláusulas generales para excluir toda responsabilidad, modificar unilateralmente derechos o eliminar activos sin una causa definida. La Ley Orgánica de Defensa del Consumidor (2000) permite examinar estipulaciones abusivas. La aceptación electrónica no convierte en válida cualquier condición impuesta por el proveedor.

La moderación de contenidos y conductas representa una función necesaria en comunidades numerosas. Las plataformas deben establecer reglas comprensibles, canales de denuncia y respuestas proporcionales. Sin embargo, la moderación puede producir responsabilidad cuando se aplica de manera arbitraria, discriminatoria o claramente insuficiente. No se exige retirar automáticamente todo contenido denunciado, pero sí valorar contexto, gravedad y evidencia. Una respuesta razonable debe proteger a la persona afectada, preservar información relevante y permitir revisión cuando la decisión perjudique significativamente a otro usuario.

El conocimiento efectivo adquiere especial importancia cuando la plataforma recibe una denuncia concreta y suficientemente fundamentada. Antes del aviso, puede resultar imposible detectar una conducta aislada. Después de conocerla, debe valorar si posee capacidad para bloquear, restringir o preservar evidencia. La inacción frente a un daño continuado puede agravar las consecuencias. Sin embargo, el conocimiento no debe presumirse por la mera existencia de grandes volúmenes de datos. La denuncia debe permitir identificar razonablemente la cuenta, conducta o contenido cuestionado.

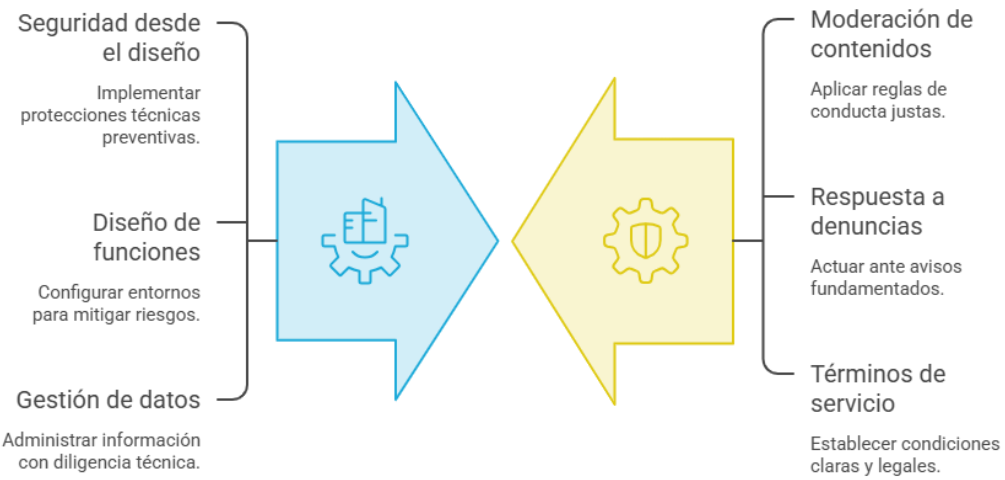
El conocimiento efectivo debe distinguirse de una obligación general de vigilar permanentemente todas las comunicaciones y conductas de los usuarios. La responsabilidad de la plataforma aumenta cuando recibe información suficientemente precisa para identificar una actividad ilícita o dañosa y, pese a disponer de capacidad técnica y jurídica para intervenir, omite actuar con diligencia. El aviso debe permitir localizar el contenido, cuenta o interacción cuestionada y aportar elementos mínimos sobre la vulneración. Una denuncia genérica no debería justificar una retirada automática, pero una comunicación fundamentada activa el deber de examinar el caso y adoptar una respuesta proporcional.

Como referencia comparada, el Reglamento de Servicios Digitales de la Unión Europea diferencia la ausencia de una obligación general de supervisión de los mecanismos de notificación y acción. Su régimen exige procedimientos accesibles para comunicar contenidos ilícitos, decisiones oportunas y explicaciones sobre las restricciones adoptadas. Este modelo resulta útil para el metaverso porque evita dos extremos: convertir a la plataforma en responsable automática de toda conducta ajena o permitirle ignorar daños identificados de manera concreta. La diligencia debe valorarse según la precisión del aviso, gravedad del riesgo, capacidad de intervención, tiempo de respuesta y protección del debido procedimiento.

La respuesta debe ser oportuna y proporcional. Un riesgo inmediato puede justificar bloqueo temporal, separación de usuarios o suspensión preventiva de una operación. Otros casos requieren investigación antes de retirar contenido o cerrar una cuenta. La plataforma debe evitar tanto la pasividad como las decisiones automáticas excesivas. Chawki et al. (2024) sostiene que los daños virtuales requieren respuestas capaces de reconocer la intensidad del entorno sin equiparar toda controversia con una agresión grave. La medida debe adecuarse al riesgo y permitir corrección posterior.

La responsabilidad puede aumentar cuando la plataforma obtiene beneficios directos de la actividad dañina. Esto puede ocurrir mediante publicidad, comisiones, venta de objetos o promoción de contenidos que generan mayor interacción. El beneficio económico no demuestra por sí solo culpabilidad, pero resulta relevante para valorar el deber de prevención. Quien diseña un modelo que incentiva conductas de riesgo y obtiene ingresos de ellas posee una posición diferente a la de un proveedor que carece de intervención. Deben analizarse incentivos, recomendaciones y mecanismos de monetización.

Figura 10
Gobernanza responsable del metaverso



Nota. La figura resume los componentes de una gobernanza responsable del metaverso, basada en seguridad, gestión de datos, moderación, atención de denuncias y condiciones transparentes. Elaboración propia.

Los sistemas automatizados de moderación pueden ayudar a gestionar grandes volúmenes de interacción, pero no sustituyen completamente la supervisión humana. Pueden interpretar incorrectamente idioma, ironía, discapacidad, gestos o contexto. Cuando una decisión afecta acceso, reputación o activos, la plataforma debe ofrecer explicación y revisión efectiva. La LOPDP (2021), artículo 20, resulta pertinente

cuando la medida se basa en valoraciones automatizadas significativas. La responsabilidad puede surgir si el operador conoce errores sistemáticos y mantiene el sistema sin correcciones razonables.

La protección de datos constituye otra fuente de obligaciones. Las plataformas determinan qué información recopilan, con qué finalidad y durante cuánto tiempo la conservan. Cuando actúan como responsables del tratamiento, deben aplicar seguridad, minimización y transparencia. Tukur et al. (2023) señalan que los entornos inmersivos generan grandes volúmenes de datos corporales y conductuales. Una filtración, acceso excesivo o reutilización incompatible puede evidenciar incumplimiento. Sin embargo, la responsabilidad debe vincularse con obligaciones concretas y no con la simple existencia de tecnología compleja.

La gestión de activos y pagos genera deberes específicos cuando la plataforma custodia saldos, ejecuta transferencias, cobra comisiones o decide la permanencia de bienes. El operador debe aplicar autenticación proporcional, alertas, trazabilidad y procedimientos de reclamación. Estas obligaciones derivan del control efectivo sobre la infraestructura y del riesgo creado por el diseño del servicio. La transparencia económica debe acompañarse de medidas técnicas capaces de impedir transferencias no autorizadas y facilitar la recuperación cuando exista fraude o uso ilegítimo de credenciales.

La cooperación con autoridades debe respetar legalidad, necesidad y proporcionalidad. La plataforma puede conservar información útil para investigar fraude, amenazas o ataques, pero no debe entregar datos indiscriminadamente ni registrar permanentemente toda interacción. La preservación debe limitarse al incidente y proteger información de terceros. Chow et al. (2023) destacan que la arquitectura distribuida dificulta localizar y asegurar registros. La responsabilidad puede surgir tanto por eliminar evidencia relevante después de una solicitud válida como por realizar una vigilancia excesiva sin fundamento suficiente.

La reparación debe adaptarse a las consecuencias del incumplimiento. Puede consistir en recuperar cuentas, restituir saldos, retirar contenido, rectificar perfiles o revisar sanciones. Una respuesta limitada a ofrecer disculpas puede resultar insuficiente cuando continúa el perjuicio. La plataforma debe corregir también los efectos derivados de datos falsos o decisiones erróneas. La reparación no implica aceptar automáticamente

toda reclamación, sino investigar de manera razonable, informar el resultado y aplicar medidas capaces de restablecer los derechos afectados.

En Ecuador, la responsabilidad de las plataformas puede fundamentarse en normas contractuales, civiles, de consumo, protección de datos y comercio electrónico. No existe un régimen único aplicable a todos los operadores del metaverso. La calificación dependerá de la relación con el usuario, el servicio ofrecido y el control sobre el riesgo. Una plataforma que dirige actividades al mercado ecuatoriano no debería excluir obligaciones mediante su ubicación extranjera. La conexión territorial debe valorarse según usuarios, efectos, tratamiento de datos y actividad económica desarrollada en el país.

El régimen aplicable debe evitar dos soluciones igualmente insuficientes: imponer al operador una vigilancia absoluta de todas las interacciones o conceder inmunidad a quien diseña, monetiza y administra el entorno. La atribución requiere valorar control efectivo, conocimiento del riesgo, previsibilidad y capacidad concreta de prevención. Las fuentes de ciberseguridad ayudan a identificar las medidas técnicas esperables, pero no reemplazan el análisis jurídico de causalidad, diligencia y reparación. Esta combinación permite distribuir responsabilidades conforme a las funciones reales de cada actor, en lugar de trasladar sistemáticamente al usuario los riesgos creados por la arquitectura.

4.4 Delitos en mundos virtuales

Los delitos cometidos en mundos virtuales deben analizarse conforme al principio de legalidad, que impide sancionar conductas no previstas expresamente por la ley penal. El hecho de que una acción ocurra mediante avatares, plataformas inmersivas o activos digitales no crea automáticamente una nueva infracción. La autoridad debe comprobar que la conducta coincide con los elementos de un tipo penal vigente, identificar al responsable y establecer la relación entre la acción digital y el resultado producido. González (2023) destaca que la valoración penal debe considerar contexto, intención y efectos verificables.

La virtualidad del medio no elimina la relevancia penal de una conducta cuando esta afecta bienes jurídicos protegidos. Una amenaza, estafa, apropiación de credenciales o ataque informático puede ejecutarse dentro del metaverso y producir consecuencias patrimoniales, emocionales o institucionales. Sin embargo, tampoco debe equipararse

toda infracción de las reglas de una plataforma con un delito. El incumplimiento de términos de servicio puede generar sanciones internas o responsabilidad contractual, mientras la intervención penal exige correspondencia estricta con una disposición del COIP (2014).

La autoría constituye uno de los principales problemas de investigación. Una conducta visible mediante un avatar no demuestra automáticamente quién la ejecutó, porque la cuenta pudo ser utilizada por otra persona, comprometida mediante un ataque o controlada parcialmente por un sistema automatizado. Pooyandeh et al. (2022) señalan que los accesos ilícitos y las vulnerabilidades de autenticación dificultan la atribución. La investigación debe combinar registros de acceso, dispositivos, credenciales, comunicaciones y circunstancias contextuales, evitando identificar al responsable únicamente por el nombre de usuario.

La estafa puede producirse cuando una persona utiliza engaño para obtener un beneficio patrimonial en perjuicio de otra. Dentro del metaverso puede manifestarse mediante venta de activos inexistentes, simulación de inversiones, falsificación de identidad o promesas sobre bienes que carecen de utilidad real. El COIP (2014), artículo 186, exige comprobar engaño, error, disposición patrimonial y perjuicio. La apariencia tridimensional, la reputación del avatar o la utilización de un contrato inteligente pueden formar parte del engaño, pero no sustituyen la prueba de los elementos del delito.

La apropiación fraudulenta por medios electrónicos puede resultar pertinente cuando el responsable utiliza sistemas informáticos para apoderarse de fondos, activos o información patrimonial. El COIP (2014), artículo 190, permite analizar transferencias ejecutadas mediante credenciales obtenidas ilícitamente, manipulación de cuentas o procedimientos electrónicos engañosos. Varela et al. (2025) advierten que la inteligencia artificial puede aumentar la credibilidad de mensajes y representaciones fraudulentas. La investigación debe establecer cómo se obtuvo el acceso y qué operaciones fueron realizadas sin autorización legítima.

Los ataques contra sistemas informáticos constituyen otra categoría relevante. Un responsable puede introducir código malicioso, alterar funciones, interrumpir servicios o destruir información dentro de una plataforma. El COIP (2014), artículo 232, sanciona determinadas afectaciones a la integridad de sistemas informáticos. Pooyandeh et al. (2022) explican que los entornos virtuales amplían la superficie de ataque por la

conexión entre servidores, aplicaciones, dispositivos y activos. La existencia de una falla no demuestra por sí sola delito; debe acreditarse intervención ilícita e intención conforme al tipo aplicable.

El acceso no consentido a sistemas, cuentas o dispositivos puede permitir apropiarse de identidades, conversaciones y activos. El COIP (2014), artículo 234, resulta aplicable cuando una persona ingresa o permanece sin autorización en un sistema protegido. La gravedad puede aumentar si el acceso permite realizar transferencias, modificar perfiles o obtener datos sensibles. La investigación debe diferenciar entre fallos de autenticación, uso de credenciales compartidas y acceso deliberadamente ilícito. La existencia de una contraseña no es el único criterio para establecer que el acceso estaba jurídicamente prohibido.

Tabla 11
Conductas delictivas que pueden presentarse en mundos virtuales

Conducta virtual	**Posible figura penal**	**Elemento principal que debe probarse**	**Evidencia relevante**
Venta de activo inexistente	Estafa	Engaño y perjuicio patrimonial	Oferta, pagos y comunicaciones
Transferencia desde cuenta ajena	Apropiación fraudulenta	Uso ilícito de medios electrónicos	Accesos y transacciones
Ingreso a perfil protegido	Acceso no consentido	Ausencia de autorización	Credenciales y registros
Alteración de plataforma	Ataque a sistemas	Daño o afectación informática	Logs y análisis técnico
Captura de comunicaciones	Interceptación ilegal	Acceso indebido al contenido	Registros y dispositivos
Difusión de base de datos	Revelación ilegal	Obtención y divulgación no autorizada	Archivos y destinatarios
Amenaza mediante avatar	Delito contra la integridad o libertad	Seriedad e idoneidad intimidatoria	Mensajes y contexto
Clonación para obtener dinero	Estafa o apropiación electrónica	Identidad falsa y beneficio	Contenido sintético y pagos
Fraude con NFT	Estafa u otra figura patrimonial	Engaño sobre autenticidad o derechos	Token, licencia y oferta
Uso de malware inmersivo	Delito informático	Introducción deliberada de código	Código, dispositivos y efectos

Nota. La calificación depende de los elementos comprobados y no de la denominación tecnológica utilizada por los participantes.

La interceptación ilegal puede producirse cuando una persona accede, registra o desvía comunicaciones sin autorización. En el metaverso, las conversaciones pueden desarrollarse mediante voz, texto, video o señales transmitidas por dispositivos. El COIP (2014), artículo 230, protege determinadas comunicaciones y datos frente a accesos ilícitos. La investigación debe establecer si existía una expectativa legítima de reserva, qué mecanismo se utilizó y quién obtuvo el contenido. No toda observación en un espacio público constituye interceptación, pero una sala restringida puede recibir una protección diferente.

La revelación ilegal de bases de datos puede presentarse cuando información de usuarios es obtenida y difundida sin autorización. El COIP (2014), artículo 229, puede resultar pertinente frente a filtraciones de perfiles, credenciales, registros biométricos o historiales de actividad. Sorrentino y López (2025) señalan que los entornos inmersivos generan información especialmente sensible por su capacidad de identificar e inferir características personales. La relevancia penal dependerá del acceso, divulgación, intención y afectación, además de las responsabilidades administrativas derivadas de la protección de datos.

Las amenazas realizadas mediante avatares deben valorarse según contenido, contexto y capacidad para generar temor razonable. Una expresión agresiva durante una actividad ficticia no constituye necesariamente un delito, pero el contexto lúdico tampoco neutraliza una amenaza seria. González (2023) destaca que las emociones y percepciones generadas en entornos virtuales influyen en la experiencia de la víctima. Deben considerarse reiteración, información personal conocida, cercanía con el autor y posibilidad de trasladar la conducta al mundo físico.

La violencia sexual virtual plantea problemas de tipicidad y valoración del daño. Algunas conductas pueden involucrar contacto simulado, representaciones sexuales no consentidas, persecución o difusión de contenido íntimo. Chawki et al. (2024) sostiene que estas experiencias pueden producir afectaciones reales, pero su calificación penal debe respetar estrictamente los elementos previstos por la legislación. No toda interacción invasiva encajará en una figura penal existente. En ciertos casos, la respuesta puede corresponder a responsabilidad civil, protección de datos, moderación o medidas administrativas.

Los delitos contra menores requieren una atención reforzada. Los agresores pueden utilizar avatares ficticios, regalos virtuales, comunicaciones privadas o identidades sintéticas para generar confianza y obtener información o contenido. Varela et al. (2025) advierten que la inteligencia artificial facilita la creación de perfiles convincentes y mensajes personalizados. La investigación debe preservar comunicaciones, identificar cuentas relacionadas y proteger la intimidad del menor. La respuesta penal debe coordinarse con medidas inmediatas de bloqueo, apoyo y protección para evitar que el daño continúe.

Los fraudes vinculados con NFT y activos digitales deben analizarse según la conducta económica concreta. La tokenización no autorizada, la falsedad sobre autenticidad, la simulación de derechos y la manipulación de precios pueden integrar modalidades distintas de engaño. Varela et al. (2025) muestran que las herramientas digitales y la inteligencia artificial amplían la capacidad de crear identidades, contenidos y ofertas fraudulentas. La calificación penal debe apoyarse en el COIP (2014) y en la prueba del engaño, el perjuicio, la apropiación o la conducta informática efectivamente ejecutada.

La inteligencia artificial puede utilizarse para clonar voces, generar rostros y automatizar comunicaciones fraudulentas. Estas herramientas aumentan la escala y credibilidad de las conductas, pero no crean por sí mismas una categoría penal diferente. Varela et al. (2025) explican que la IA amplía las capacidades de la ciberdelincuencia y dificulta la detección. La investigación debe identificar quién proporcionó instrucciones, controló el sistema y obtuvo el beneficio. La responsabilidad no corresponde al programa, sino a las personas que lo emplearon deliberadamente.

La tentativa también puede presentarse cuando el autor inicia actos dirigidos a cometer un delito, pero no logra consumarlo. Una transferencia puede ser bloqueada, una víctima puede detectar el engaño o una plataforma puede suspender una cuenta antes de producirse el perjuicio. La valoración debe determinar si existió inicio de ejecución y si la falta de consumación obedeció a circunstancias ajenas a la voluntad del responsable. Los simples preparativos, como crear un avatar ficticio, no siempre son suficientes para configurar responsabilidad penal.

La participación de varias personas puede adoptar formas de autoría, coautoría o complicidad. Un individuo puede crear contenido falso, otro proporcionar credenciales y un tercero recibir los fondos. También pueden intervenir grupos organizados que

utilizan múltiples cuentas y plataformas. La distribución de tareas no elimina la responsabilidad individual, pero exige demostrar el aporte y conocimiento de cada participante. Los registros técnicos pueden mostrar conexiones entre cuentas, aunque deben complementarse con evidencia contextual que permita distinguir colaboración consciente de coincidencias o servicios legítimos.

La responsabilidad penal de las personas jurídicas dependerá de los supuestos expresamente previstos por el ordenamiento. No debe presumirse que una plataforma responde penalmente por todo delito cometido por usuarios. Sin embargo, pueden existir responsabilidades de sus representantes o de la propia entidad cuando se cumplan los requisitos legales correspondientes. La omisión de medidas de seguridad también puede generar consecuencias civiles, administrativas o contractuales. Es necesario separar cuidadosamente la responsabilidad penal del autor de la posible responsabilidad de la empresa por incumplimientos propios.

La preservación de evidencia resulta decisiva para investigar delitos virtuales. Deben conservarse de manera proporcional comunicaciones, registros de acceso, direcciones, transacciones, archivos y metadatos vinculados con el incidente. La plataforma debe evitar alteraciones y documentar quién accedió a la información. Sin embargo, la investigación penal no autoriza recopilar indefinidamente toda la actividad de los usuarios. La evidencia debe limitarse a los hechos relevantes, proteger datos de terceros y respetar los procedimientos legales que garanticen autenticidad y defensa.

4.5 Acoso y violencia mediante avatares

El acoso y la violencia mediante avatares comprenden conductas reiteradas o intensas dirigidas contra una persona dentro de entornos virtuales, capaces de afectar su dignidad, seguridad, libertad o bienestar. Pueden manifestarse mediante insultos, persecución, aproximaciones invasivas, amenazas, exclusión, difusión de contenidos y simulación de contacto corporal. La ausencia de proximidad física entre agresor y víctima no elimina la relevancia de la experiencia. La valoración debe considerar el grado de inmersión, la persistencia de la conducta y sus consecuencias verificables (Chawki et al., 2024).

El acoso virtual suele caracterizarse por la reiteración, aunque una sola conducta especialmente grave también puede producir una afectación significativa. Un usuario puede seguir al avatar de la víctima entre diferentes espacios, enviar mensajes

constantes, interrumpir actividades o reaparecer mediante nuevas cuentas después de un bloqueo. Munn y Weijers (2023) señalan que la persistencia de los mundos virtuales puede intensificar la sensación de vigilancia y pérdida de control. La conducta debe examinarse según frecuencia, duración, intencionalidad y capacidad real de la víctima para evitarla.

La persecución del avatar constituye una modalidad específica de hostigamiento. El agresor puede acompañar a la persona de forma continua, invadir su espacio virtual o impedirle participar normalmente en determinadas actividades. Aunque la víctima pueda desconectarse, abandonar la plataforma no siempre representa una solución adecuada cuando allí mantiene relaciones, estudios, trabajo o activos. Obligarla a retirarse traslada las consecuencias de la agresión a quien la sufre. La plataforma debe ofrecer herramientas que permitan bloquear al responsable sin perder completamente el acceso al entorno.

Los insultos, expresiones degradantes y mensajes discriminatorios pueden dirigirse tanto a características reales como a rasgos elegidos para el avatar. La conducta puede relacionarse con género, etnia, discapacidad, edad, nacionalidad o identidad cultural. No toda expresión ofensiva constituye jurídicamente acoso, pero la reiteración, el contexto y la finalidad de excluir o humillar pueden aumentar su gravedad. González (2023) destaca que la percepción emocional de la víctima debe valorarse junto con la intención, el contenido y las consecuencias producidas por la conducta virtual.

La violencia sexual mediante avatares puede incluir aproximaciones no consentidas, gestos sexualizados, simulaciones de contacto, difusión de escenas íntimas o utilización de dispositivos hápticos. Chawki et al. (2024) advierte que estas experiencias pueden ocasionar daños reales, especialmente cuando la inmersión genera una fuerte sensación de presencia. Sin embargo, la calificación jurídica debe respetar las categorías legales vigentes y no equiparar automáticamente toda interacción virtual con una agresión física. Pueden concurrir respuestas penales, civiles, administrativas, contractuales o de moderación.

El consentimiento representa un elemento fundamental para diferenciar interacción permitida y conducta invasiva. Aceptar participar en un mundo virtual, utilizar dispositivos hápticos o ingresar a un espacio social no supone autorizar cualquier contacto. Sakka et al. (2026) sostienen que los límites digitales deben poder expresarse,

modificarse y retirarse durante la experiencia. La plataforma debe permitir configurar proximidad, contacto, voz y estímulos sensoriales. La autorización concedida para una actividad concreta no debe interpretarse como consentimiento general, permanente o extensible a otros participantes.

La arquitectura tecnológica puede prevenir o facilitar situaciones de acoso. Las zonas personales, el bloqueo, el silenciamiento, la salida rápida y la restricción de mensajes ofrecen protección inmediata. En cambio, los espacios cerrados sin controles, la localización constante y la dificultad para bloquear usuarios incrementan la vulnerabilidad. Chawki et al. (2024) destaca que la respuesta frente al acoso virtual debe considerar el diseño de la plataforma y la intensidad de la experiencia inmersiva, además de la conducta individual del agresor.

Tabla 12
Modalidades de acoso y violencia mediante avatares

Modalidad	Manifestación virtual	Elemento de gravedad	Respuesta inmediata
Persecución	Seguimiento persistente entre espacios	Reiteración y dificultad para evitar al agresor	Bloqueo y separación
Insultos reiterados	Mensajes, voz o gestos degradantes	Frecuencia y finalidad de humillar	Silenciamiento y revisión
Violencia sexual	Contacto o representación no consentida	Ausencia de consentimiento e inmersión	Interrupción y preservación de evidencia
Amenazas	Expresiones destinadas a intimidar	Credibilidad y conocimiento de datos personales	Restricción y evaluación urgente
Exclusión discriminatoria	Impedimento de acceso o participación	Motivo protegido y efecto colectivo	Restablecimiento y sanción
Difusión íntima	Publicación de imágenes o escenas privadas	Falta de autorización y alcance	Retiro urgente
Hostigamiento grupal	Ataques coordinados por varios usuarios	Número de participantes y continuidad	Protección y análisis conjunto
Contacto háptico invasivo	Estímulos físicos no aceptados	Intensidad y control del usuario	Desactivación inmediata

Modalidad	Manifestación virtual	Elemento de gravedad	Respuesta inmediata
Acoso mediante cuentas nuevas	Reaparición después de sanciones	Evasión deliberada de medidas	Vinculación y restricción reforzada
Violencia contra menores	Captación, sexualización o manipulación	Edad y relación desigual	Intervención prioritaria

Nota. Las respuestas deben considerar la intensidad, la reiteración y la vulnerabilidad de la persona afectada.

Las amenazas deben valorarse según su contenido, contexto y capacidad para producir temor razonable. Una expresión formulada durante una actividad ficticia puede formar parte de la narrativa, mientras otra puede revelar información personal o anunciar una acción concreta fuera de la plataforma. González (2023) destaca que la experiencia emocional no puede separarse del contexto tecnológico. La plataforma debe analizar identidad conocida, reiteración, acceso a datos personales y antecedentes entre las partes antes de determinar la gravedad y aplicar una medida.

El hostigamiento grupal puede intensificar el daño cuando varios participantes coordinan insultos, denuncias falsas, exclusión o persecución. La víctima puede experimentar una pérdida total de control sobre su participación y reputación. La respuesta no debería limitarse a examinar cada mensaje aisladamente, pues la gravedad deriva del patrón conjunto. Chawki et al. (2024) señala que la persistencia y amplificación digital pueden transformar conductas individuales en agresiones colectivas. La plataforma debe identificar conexiones, coordinación y repetición sin convertir toda coincidencia en prueba automática de organización.

La difusión no consentida de imágenes, conversaciones o escenas íntimas puede prolongar el daño debido a la facilidad de copiar, descargar y trasladar contenidos. La víctima puede perder control incluso después de que el archivo original sea retirado. La respuesta debe priorizar el cese de circulación, la restricción de copias y la protección de identidad. La preservación probatoria no exige mantener el contenido públicamente disponible. Puede conservarse una copia restringida, accesible únicamente para investigación y durante el tiempo necesario, aplicando confidencialidad y seguridad.

La accesibilidad del sistema de denuncia condiciona la eficacia de la protección. Obligar a la persona afectada a abandonar el entorno, recorrer menús complejos o formular jurídicamente el incidente puede prolongar la exposición y desalentar el

reclamo. El mecanismo debería ofrecer categorías comprensibles, permitir adjuntar registros y confirmar la recepción de la comunicación. También debe informar qué medida provisional fue adoptada y cómo se desarrollará la revisión. Cuando el riesgo era identificable y existían medios razonables para intervenir, la ausencia de respuesta puede constituir un indicio de falta de diligencia.

La moderación automatizada puede detectar palabras, movimientos o patrones asociados con violencia, pero posee limitaciones para interpretar contexto, ironía y consentimiento. Un gesto puede ser ofensivo en una situación y legítimo en otra. Las personas con discapacidad también pueden realizar movimientos que el sistema clasifique erróneamente. La revisión humana resulta necesaria cuando la medida afecta significativamente cuentas o reputaciones. El moderador debe analizar secuencia, relación entre participantes y posibles fallos técnicos, evitando aceptar de manera automática la clasificación generada por el algoritmo.

Las medidas frente al agresor deben guardar proporcionalidad con la conducta. Pueden incluir advertencia, silenciamiento, separación espacial, restricción temporal, suspensión o cancelación definitiva. Una amenaza grave o violencia sexual puede justificar intervención inmediata, mientras un conflicto aislado puede requerir una respuesta menos intensa. Chawki et al. (2024) sostiene que la protección debe reconocer la gravedad de los daños virtuales sin aplicar sanciones uniformes. La revisión posterior permite corregir errores, pero no debe retrasar medidas necesarias para detener una afectación continuada.

La protección de menores exige procedimientos reforzados porque pueden tener mayores dificultades para reconocer manipulación, pedir ayuda o conservar evidencia. Los agresores pueden presentarse mediante avatares juveniles, ofrecer regalos y trasladar la conversación hacia espacios privados. La plataforma debe restringir contactos, identificar patrones de captación y activar moderación especializada. La respuesta debe proteger la intimidad del menor y evitar que repita innecesariamente el relato. También debe coordinarse con representantes y autoridades cuando existan indicios fundados de una conducta grave.

La prueba del acoso puede incluir mensajes, grabaciones, movimientos, listas de bloqueo, reportes y testimonios. Sin embargo, la víctima no debe asumir por sí sola toda la carga de documentación. La plataforma conserva registros técnicos que pueden

demostrar reiteración, uso de cuentas sucesivas y coincidencias de dispositivos. La conservación debe activarse ante una denuncia fundada y limitarse a información pertinente. Registrar permanentemente toda conversación o contacto generaría una vigilancia desproporcionada y podría crear nuevos riesgos para quienes participan legítimamente en el entorno.

La reparación puede comprender retiro de contenidos, restablecimiento de acceso, corrección de sanciones, protección frente a nuevas cuentas y compensación por daños. En casos reputacionales, debe eliminarse la asociación entre la víctima y conductas que le fueron falsamente atribuidas. Cuando existe afectación psicológica, pueden requerirse medidas de apoyo. La reparación no debe limitarse a sancionar al agresor, sino procurar que la persona afectada recupere condiciones seguras de participación. La posibilidad de permanecer en la plataforma forma parte del restablecimiento cuando ese espacio posee importancia social o profesional.

El acoso y la violencia mediante avatares requieren, en definitiva, una respuesta que combine diseño preventivo, moderación contextual, conservación proporcional de evidencia y reparación efectiva. La virtualidad no convierte estas conductas en irrelevantes, pero tampoco permite calificarlas sin examinar contexto, consentimiento e intensidad. Chawki et al. (2024), González (2023) y Sakka et al. (2026) ofrecen fundamentos pertinentes para comprender sus dimensiones jurídicas, emocionales y tecnológicas, evitando recurrir a fuentes sobre NFT o modelos económicos que no analizan estas formas de violencia.

4.6 Suplantación, fraude y activos digitales

La suplantación de identidad en el metaverso ocurre cuando una persona utiliza sin autorización los rasgos, credenciales, voz, imagen, avatar o información de otra con la finalidad de aparentar que actúa en su nombre. Esta conducta puede afectar patrimonio, reputación, privacidad y seguridad. La facilidad para modificar representaciones digitales permite crear perfiles altamente convincentes, especialmente cuando se combinan datos personales con herramientas de inteligencia artificial. Sorrentino y López (2025) advierten que los entornos inmersivos amplían las posibilidades de identificación y, simultáneamente, los riesgos de apropiación de la identidad.

La apropiación de una cuenta constituye una de las formas más frecuentes de suplantación. Puede producirse mediante robo de contraseñas, phishing, malware,

reutilización de credenciales o vulnerabilidades de autenticación. Una vez dentro, el responsable puede comunicarse con contactos, transferir activos, modificar datos o utilizar la reputación de la víctima. Pooyandeh et al. (2022) señalan que la integración entre plataformas, dispositivos y servicios incrementa la superficie de ataque. La protección debe incluir autenticación reforzada, alertas de acceso y procedimientos eficaces de recuperación.

La clonación de voz y rostro mediante inteligencia artificial permite generar mensajes, videollamadas o representaciones aparentemente auténticas. Estas herramientas pueden utilizarse para solicitar dinero, obtener credenciales o inducir decisiones patrimoniales. Varela et al. (2025) explican que la inteligencia artificial incrementa la capacidad de los ciberdelincuentes para producir contenidos personalizados y creíbles. La investigación debe identificar no solo el archivo sintético, sino también quién lo creó, distribuyó y utilizó para obtener un beneficio o causar un perjuicio.

La copia de avatares también puede generar suplantación cuando la representación permite identificar razonablemente a una persona. No todo parecido visual constituye una infracción, pues algunos diseños utilizan elementos comunes. La relevancia aumenta cuando se reproducen nombre, voz, movimientos, vestimenta distintiva o relaciones sociales con la finalidad de engañar. Castillo et al. (2024) destacan que la identidad digital se construye mediante múltiples atributos vinculados. La valoración debe considerar el conjunto de elementos y no limitarse a comparar únicamente la apariencia gráfica.

El fraude se configura cuando una persona emplea engaño para obtener un beneficio económico y provocar una disposición patrimonial perjudicial. En el metaverso puede manifestarse mediante ventas falsas, inversiones simuladas, promesas de rentabilidad, clonación de perfiles o utilización de contratos aparentemente legítimos. El COIP (2014), artículo 186, exige comprobar engaño, error, disposición patrimonial y perjuicio. La utilización de tecnología avanzada no sustituye estos elementos, aunque puede aumentar la credibilidad de la maniobra y dificultar la identificación del responsable.

Los activos digitales pueden ser utilizados como objeto, instrumento o resultado del fraude. Un responsable puede vender un activo inexistente, ofrecer derechos que no posee o transferir un token previamente sustraído. Martínez et al. (2024) señalan que la

confusión entre token, archivo y derechos asociados facilita ofertas engañosas. El comprador puede creer que adquiere propiedad intelectual, exclusividad o acceso permanente cuando recibe únicamente un identificador técnico. La información sobre el activo debe diferenciar claramente cada componente y las facultades efectivamente transferidas.

El fraude con NFT puede consistir en tokenizar obras ajenas, falsificar la identidad del creador, manipular precios o simular una comunidad inexistente. Madanchian y Taherdoost (2024) explica que el valor de estos activos depende de confianza, reputación y sostenibilidad del modelo económico. Cuando la oferta crea artificialmente escasez o promete rentabilidad segura, puede inducir decisiones patrimoniales basadas en información falsa. Sin embargo, la pérdida económica derivada únicamente de la volatilidad del mercado no demuestra fraude si los riesgos fueron informados y no existió engaño.

El phishing inmersivo puede reproducir tiendas, oficinas, eventos o interfaces conocidas para capturar credenciales y datos de pago. La experiencia tridimensional puede aumentar la confianza porque el usuario reconoce elementos visuales, voces o avatares familiares. Fiaz et al. (2024) destacan que la identidad y la autenticación constituyen componentes críticos de la seguridad del metaverso. Las plataformas deben verificar enlaces, advertir sobre espacios no oficiales y evitar que diseños falsos reproduzcan de manera indistinguible funciones sensibles como inicio de sesión o confirmación de pagos.

Los contratos inteligentes también pueden utilizarse de forma fraudulenta. Un código malicioso puede aparentar una compra legítima mientras autoriza transferencias adicionales o concede permisos permanentes. La ejecución automática no convierte la operación en válida si existió engaño, error o ausencia de consentimiento. Pooyandeh et al. (2022) señalan que las vulnerabilidades técnicas pueden ser explotadas para alterar operaciones. El usuario debe conocer qué permisos concede, qué activos pueden transferirse y cómo revocar autorizaciones antes de interactuar con programas desconocidos.

La manipulación de mercado puede realizarse mediante compras coordinadas entre cuentas relacionadas, ofertas ficticias y promoción engañosa. Estas prácticas crean una apariencia artificial de demanda y pueden inducir a terceros a pagar precios elevados.

Madanchian y Taherdoost (2024) explica que la confianza y la transparencia son determinantes para la sostenibilidad de los mercados de NFT. La valoración jurídica debe examinar relaciones entre cuentas, frecuencia de operaciones, control del emisor, información publicitaria y beneficios obtenidos, sin presumir legitimidad por el solo registro de las transacciones.

La apropiación fraudulenta por medios electrónicos puede presentarse cuando el responsable utiliza credenciales o sistemas para transferir activos sin autorización. El COIP (2014), artículo 190, permite examinar operaciones ejecutadas mediante medios informáticos que ocasionan perjuicio patrimonial. La cadena de bloques puede registrar la transferencia, pero no demuestra que exista consentimiento legítimo. Una operación técnicamente válida puede provenir de una cuenta comprometida. La investigación debe reconstruir cómo se obtuvo el acceso, quién recibió el activo y qué medidas se adoptaron para ocultar su origen.

La recuperación de activos digitales sustraídos puede resultar difícil por la rapidez de las transferencias y la utilización de múltiples cuentas. Los tokens pueden pasar por diferentes plataformas, convertirse en otros activos o enviarse a servicios que dificultan su rastreo. La trazabilidad distribuida facilita seguir movimientos, pero no siempre identificar a las personas. Pooyandeh et al. (2022) destacan que la investigación requiere combinar análisis técnico con información de plataformas, dispositivos y medios de pago. La restitución puede exigir cooperación entre operadores y autoridades de varias jurisdicciones.

Las plataformas deben implementar procedimientos para detectar accesos anómalos, transferencias inusuales y creación masiva de perfiles. Sin embargo, la detección automatizada no debe bloquear indiscriminadamente a usuarios legítimos. Las medidas deben valorar ubicación, dispositivo, comportamiento y riesgo económico. Fiaz et al. (2024) señalan que una gestión adecuada de identidad requiere autenticación y control continuo. Cuando existe una operación sospechosa, puede resultar razonable solicitar confirmación adicional, retrasar temporalmente la transferencia o permitir una revisión rápida antes de su ejecución definitiva.

La protección de la víctima exige recuperar la cuenta, impedir nuevas transferencias y corregir mensajes emitidos mediante la identidad suplantada. La respuesta no debe limitarse a cambiar la contraseña si persisten sesiones activas, permisos concedidos o

contenidos falsos. También puede ser necesario informar a contactos, retirar perfiles duplicados y preservar evidencia. Sorrentino y López (2025) destacan que la afectación de identidad puede prolongarse mediante registros e inferencias. La reparación debe restablecer tanto el control técnico como la confianza vinculada con la representación digital.

La prueba puede incluir historiales de acceso, transacciones, mensajes, grabaciones, archivos sintéticos, direcciones digitales y datos de dispositivos. Los metadatos permiten identificar fechas, herramientas y secuencias, aunque pueden alterarse o resultar incompletos. La evidencia debe preservarse con integridad y documentar quién la obtuvo y manipuló. La cadena de bloques puede demostrar que una transferencia ocurrió, pero no quién actuó físicamente ni si existía autorización. Debe combinarse con autenticación, comunicaciones y circunstancias económicas del caso.

La prevención requiere educación digital, diseño seguro y mecanismos de verificación. Los usuarios deben desconfiar de solicitudes urgentes, confirmar identidades mediante canales alternativos y revisar permisos antes de aprobar operaciones. Las plataformas deben ofrecer autenticación multifactor, alertas, límites de transferencia y verificación de emisores. Castillo et al. (2024) sostienen que la identidad digital exige controles capaces de proteger sus diferentes atributos. La seguridad no puede depender exclusivamente de la diligencia individual cuando el operador controla la arquitectura y conoce los riesgos recurrentes.

La suplantación, el fraude y los activos digitales deben analizarse de manera conjunta cuando el engaño utiliza identidades virtuales para producir consecuencias patrimoniales. Varela et al. (2025), Fiaz et al. (2024) y Castillo et al. (2024) permiten comprender la combinación de identidades sintéticas, apropiación de credenciales y operaciones engañosas. La investigación debe diferenciar el acceso ilegítimo, la falsificación de representaciones, la oferta patrimonial y la transferencia del activo, evitando que la complejidad tecnológica oculte la secuencia de conductas relevantes.

4.7 Ciberseguridad en entornos inmersivos

La ciberseguridad en entornos inmersivos comprende medidas destinadas a proteger cuentas, dispositivos, comunicaciones, datos y activos frente a accesos no autorizados, alteraciones, interrupciones o apropiaciones ilícitas. El metaverso amplía la superficie de ataque porque integra plataformas, sensores, redes, servicios en la nube y sistemas

automatizados. Pooyandeh et al. (2022), Chow et al. (2023) y Gupta et al. (2023) permiten analizar estas amenazas desde la infraestructura, la visualización y los modelos de confianza cero.

La arquitectura del metaverso combina múltiples componentes interdependientes. Visores, controladores, aplicaciones, redes, servidores y contratos inteligentes intercambian información de manera continua. Un atacante puede aprovechar el elemento menos protegido para ingresar al resto del sistema. Gupta et al. (2023) destacan que los modelos tradicionales basados únicamente en la confianza interna resultan insuficientes frente a entornos distribuidos. La protección requiere verificar identidades, dispositivos y permisos en cada acceso, aplicando el principio de confianza mínima y controles diferenciados según el nivel de riesgo.

La identidad digital constituye uno de los principales objetivos de los ataques. El control de una cuenta puede permitir suplantar al usuario, acceder a conversaciones, retirar activos o perjudicar su reputación. Fiaz et al. (2024) señalan que la autenticación debe adaptarse a interacciones persistentes y a múltiples dispositivos. Las contraseñas por sí solas resultan insuficientes cuando existen operaciones patrimoniales o datos sensibles. Se requieren autenticación multifactor, alertas de acceso, gestión segura de sesiones y procedimientos eficaces para recuperar cuentas comprometidas.

La autenticación biométrica puede aumentar la seguridad mediante reconocimiento facial, ocular, vocal o conductual, pero también crea riesgos cuando los datos son almacenados de manera inadecuada. Una contraseña puede modificarse después de una filtración, mientras una característica biométrica permanece vinculada con la persona. Fiaz et al. (2024) advierten que los entornos inmersivos recopilan señales corporales con alta capacidad identificativa. Estos datos deben cifrarse, minimizarse y utilizarse únicamente para finalidades justificadas, evitando que la autenticación se transforme en vigilancia permanente.

Los dispositivos inmersivos pueden ser vulnerables a software malicioso, alteración de sensores y acceso remoto. Un ataque puede modificar lo que el usuario observa, generar desorientación o inducir acciones equivocadas. Pooyandeh et al. (2022) explican que la conexión entre hardware y software introduce riesgos capaces de afectar seguridad digital y física. Los fabricantes deben aplicar actualizaciones, pruebas y mecanismos de arranque seguro. El usuario también necesita recibir advertencias claras cuando un

dispositivo deja de recibir soporte o presenta vulnerabilidades conocidas que comprometen su funcionamiento.

La protección de las comunicaciones resulta esencial porque los usuarios intercambian voz, texto, video y movimientos dentro de espacios privados y públicos. Un tercero puede interceptar, modificar o reproducir estos contenidos para cometer fraude o afectar la intimidad. Chow et al. (2023) destacan que las arquitecturas distribuidas dificultan garantizar confidencialidad e integridad de extremo a extremo. El cifrado debe acompañarse de controles de acceso y autenticación, pues una comunicación protegida técnicamente continúa siendo vulnerable si una de las cuentas participantes ha sido comprometida.

La seguridad de los activos digitales requiere mecanismos capaces de prevenir transferencias no autorizadas y pérdida de credenciales. Los contratos inteligentes y las cadenas de bloques ofrecen trazabilidad, pero no corrigen automáticamente el fraude. Una operación puede quedar registrada de manera inmutable, aunque haya sido ejecutada desde una cuenta sustraída. Gupta et al. (2023) sostienen que cada solicitud debe evaluarse según identidad, dispositivo y contexto. Las plataformas pueden incorporar límites, confirmaciones adicionales, alertas y pausas temporales frente a movimientos anómalos o de elevado valor.

Tabla 13
Riesgos de ciberseguridad en entornos inmersivos y medidas de control

Riesgo	Componente afectado	Posible consecuencia	Medida de control
Robo de credenciales	Cuenta de usuario	Suplantación y pérdida de activos	Autenticación multifactor
Malware inmersivo	Dispositivo y aplicación	Alteración de experiencia y datos	Actualización y verificación de software
Interceptación	Voz, texto y video	Divulgación o manipulación	Cifrado y control de acceso
Ataque a sensores	Visor y controladores	Desorientación o seguimiento	Validación y aislamiento del dispositivo
Transferencia fraudulenta	Billetera o saldo virtual	Pérdida patrimonial	Confirmaciones y límites
Contrato inteligente vulnerable	Operación automatizada	Desvío de fondos	Auditoría de código

Riesgo	Componente afectado	Posible consecuencia	Medida de control
Filtración biométrica	Datos corporales	Suplantación persistente	Cifrado y minimización
Denegación de servicio	Plataforma o servidor	Interrupción de actividades	Redundancia y respuesta a incidentes
Cuenta privilegiada comprometida	Administración	Acceso masivo y alteraciones	Control estricto de privilegios
Ingeniería social	Usuario y soporte	Entrega voluntaria de datos	Formación y verificación alternativa

Nota. La seguridad debe combinar controles técnicos, organizacionales y humanos adaptados al nivel de riesgo.

Los contratos inteligentes pueden contener errores de programación o funciones ocultas capaces de transferir activos sin autorización suficiente. Una vez desplegado el código, corregirlo puede resultar complejo, especialmente cuando se presenta como inmutable. Pooyandeh et al. (2022) destacan que la automatización amplía los efectos de una vulnerabilidad, pues el daño puede ejecutarse rápidamente. Antes de utilizar estos programas deben realizarse auditorías, pruebas, revisión de permisos y mecanismos de pausa. La transparencia del código no garantiza que todos los usuarios puedan comprender sus consecuencias.

Los ataques de denegación de servicio pueden impedir el acceso a espacios virtuales, actividades laborales, eventos o servicios esenciales. La interrupción puede generar pérdidas económicas, afectar comunicaciones y bloquear temporalmente activos. Chow et al. (2023) señalan que la distribución de infraestructura mejora resiliencia, aunque también complica coordinación y recuperación. Las plataformas deben contar con redundancia, monitoreo y procedimientos de continuidad. La obligación no consiste en garantizar disponibilidad absoluta, sino en reducir interrupciones previsibles y restablecer el servicio en plazos razonables.

Las cuentas administrativas representan objetivos especialmente sensibles porque poseen permisos para modificar reglas, acceder a datos o suspender usuarios. Si una cuenta privilegiada es comprometida, el atacante puede producir daños masivos. Gupta et al. (2023) recomiendan aplicar acceso de privilegio mínimo, segmentación y verificación continua. Ningún administrador debería conservar facultades superiores a las necesarias. Las operaciones críticas deben requerir confirmación adicional, registro

detallado y, cuando sea posible, intervención de más de una persona para evitar abusos o errores individuales.

La ingeniería social continúa siendo efectiva, aunque la infraestructura tecnológica sea avanzada. Los atacantes pueden utilizar avatares confiables, espacios falsos, mensajes urgentes o voces clonadas para persuadir al usuario de entregar credenciales. Varela et al. (2025) explican que la inteligencia artificial permite personalizar engaños y aumentar su credibilidad. La prevención requiere educación, advertencias contextuales y canales alternativos de verificación. No resulta suficiente responsabilizar al usuario cuando la plataforma permite imitaciones convincentes o carece de señales para identificar comunicaciones oficiales.

La actualización del software constituye una medida esencial para corregir vulnerabilidades conocidas. Sin embargo, también puede introducir errores, incompatibilidades o cambios que afecten dispositivos antiguos. Los proveedores deben comunicar riesgos, ofrecer instrucciones y evitar abandonar productos sin un periodo razonable de soporte. Pooyandeh et al. (2022) señalan que los ecosistemas complejos requieren coordinación entre fabricantes y desarrolladores. Una vulnerabilidad puede persistir si cada actor atribuye la responsabilidad al otro. Deben existir procedimientos claros para reportar, corregir y divulgar fallos de seguridad.

La respuesta a incidentes debe definir cómo detectar, contener, investigar y reparar un ataque. Las plataformas necesitan equipos responsables, canales de reporte y protocolos para preservar evidencia. Cuando existe una cuenta comprometida, debe ser posible cerrar sesiones, suspender transferencias y recuperar control sin eliminar información relevante. Pooyandeh et al. (2022) destacan que la respuesta debe proteger simultáneamente seguridad y privacidad. No toda amenaza justifica acceder indiscriminadamente a conversaciones o movimientos corporales. La investigación debe limitarse a los datos necesarios para comprender el incidente.

La notificación de incidentes permite que los usuarios adopten medidas frente a filtraciones o accesos indebidos. El aviso debe explicar qué ocurrió, qué información fue afectada y qué acciones se recomiendan. Ocultar una vulnerabilidad puede prolongar el daño y aumentar la responsabilidad del proveedor. Sin embargo, una comunicación prematura o imprecisa también puede generar confusión. La plataforma debe confirmar los elementos básicos, contener el riesgo y comunicar de manera

oportuna, evitando minimizar el incidente o trasladar automáticamente la culpa a las personas afectadas.

La seguridad infantil exige controles reforzados porque los menores pueden compartir información, aceptar contactos o instalar contenidos sin comprender completamente el riesgo. Los entornos dirigidos a esta población deben limitar comunicaciones privadas, compras y acceso de terceros. Varela et al. (2025) advierten que los agresores pueden utilizar inteligencia artificial para crear perfiles convincentes. La protección debe combinar verificación apropiada de edad, configuraciones seguras por defecto, supervisión proporcional y educación digital, sin recopilar más datos personales de los necesarios.

La ciberseguridad también depende de la cooperación entre plataformas, fabricantes, proveedores de identidad y autoridades. Un incidente puede comenzar en un dispositivo, extenderse a una cuenta y finalizar con la transferencia de activos hacia otra jurisdicción. Chow et al. (2023) señalan que la naturaleza distribuida exige protocolos compartidos para intercambio de alertas y preservación de registros. Esta cooperación debe contar con bases legales, límites y medidas de confidencialidad. Compartir información de seguridad no autoriza divulgar indiscriminadamente datos personales de los usuarios.

4.8 Evidencia digital y jurisdicción

La investigación de hechos ocurridos en el metaverso depende en gran medida de evidencia digital capaz de reconstruir acciones, identidades, comunicaciones y transferencias. Esta evidencia puede incluir registros de acceso, mensajes, movimientos de avatares, grabaciones, metadatos, archivos, transacciones y datos procedentes de dispositivos inmersivos. Su utilidad jurídica no depende únicamente de que exista información técnica, sino de que pueda demostrarse su autenticidad, integridad y relación con el hecho investigado. La volatilidad de estos registros exige procedimientos tempranos de identificación y preservación.

La evidencia generada por una plataforma puede encontrarse distribuida entre servidores, aplicaciones, dispositivos y proveedores externos. Una conversación puede conservarse en un sistema, mientras los datos de acceso permanecen en otro y la transacción económica se registra en una cadena de bloques. Esta fragmentación dificulta obtener una visión completa del incidente. La investigación debe identificar

qué componente produjo cada registro, quién lo administra y durante cuánto tiempo permanece disponible. La ausencia de coordinación puede provocar pérdida de información relevante antes de que una autoridad solicite formalmente su conservación.

La preservación consiste en impedir que la información sea modificada, eliminada o sobrescrita después de conocerse un incidente. Alqahtany y Syed (2024) resaltan que la preservación temprana y el registro verificable de actuaciones son esenciales para evitar alteraciones. Las plataformas suelen aplicar periodos limitados de conservación y actualizar continuamente sus bases de datos. Una denuncia fundada puede justificar la inmovilización temporal de registros directamente vinculados con el caso. Esta medida debe ser proporcional y específica. No corresponde conservar indefinidamente toda la actividad del usuario cuando solo se investiga una interacción, transferencia o acceso determinado dentro de un periodo claramente delimitado.

La integridad permite demostrar que el contenido presentado corresponde con el registro originalmente obtenido. Alqahtany y Syed (2024) proponen mecanismos basados en blockchain para documentar transferencias, preservar trazabilidad y detectar modificaciones durante el manejo forense. Estas herramientas pueden reforzar el control, pero no sustituyen la adquisición técnicamente correcta ni la valoración judicial. En el metaverso deben conservarse copias forenses, resúmenes criptográficos, marcas temporales y registros de cada intervención, evitando que la evidencia sea alterada por actualizaciones, conversiones o accesos posteriores.

Santamaría et al. (2023) muestran que los metadatos y registros de intervención permiten reconstruir la cadena de custodia. Los metadatos proporcionan información sobre creación, modificación, origen, dispositivo, ubicación aproximada y transmisión de un archivo. En un entorno inmersivo también pueden reflejar sesiones, permisos, movimientos y relación entre cuentas. Sin embargo, no deben interpretarse de forma aislada, pues pueden alterarse, resultar incompletos o depender de configuraciones incorrectas. Un registro horario no demuestra por sí solo quién realizó la conducta. La investigación debe contrastarlo con autenticación, comunicaciones, transacciones y otros elementos capaces de contextualizar el dato técnico.

La cadena de custodia documenta quién obtuvo, preservó, transfirió y analizó cada elemento probatorio. Santamaría et al. (2023) destacan que la integridad, la privacidad y la trazabilidad deben mantenerse desde la adquisición hasta la presentación judicial,

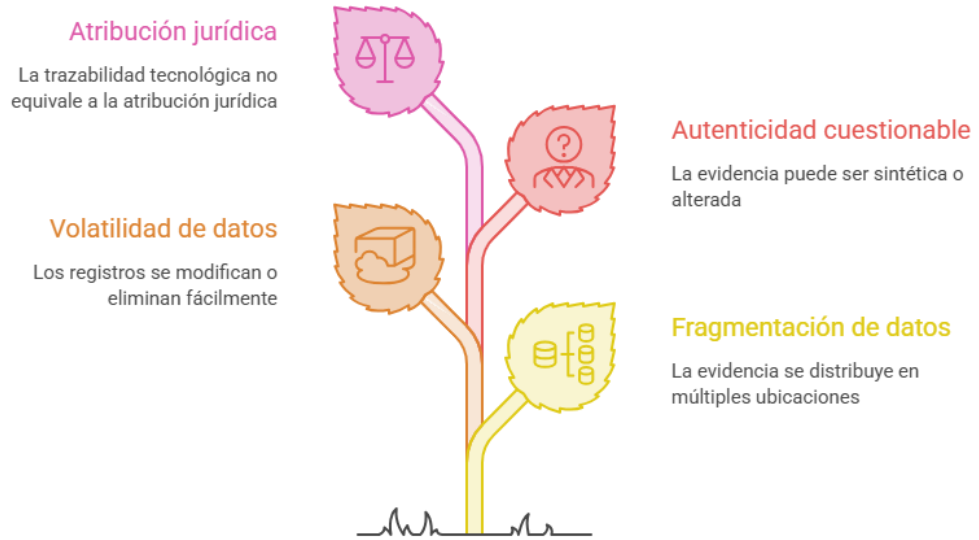
y que los registros distribuidos pueden apoyar ese objetivo cuando participan entidades independientes y procedimientos estandarizados. En el metaverso, la documentación debe incluir la versión del sistema, el método de extracción, las marcas temporales, los responsables de cada intervención y cualquier transformación aplicada al archivo original. Alqahtany y Syed (2024) destacan que la trazabilidad verificable de la preservación, adquisición, análisis y documentación permite detectar alteraciones y asignar responsabilidades durante el manejo de la evidencia.

Los registros distribuidos pueden demostrar que una transacción fue incorporada en una fecha determinada y que una dirección digital transfirió un activo a otra. No obstante, este registro no identifica necesariamente a la persona que controlaba la dirección ni demuestra que existiera consentimiento válido. Kostenko et al. (2022) advierten que la trazabilidad tecnológica debe distinguirse de la atribución jurídica. La evidencia de cadena de bloques debe complementarse con datos de acceso, dispositivos, plataformas de intercambio y comunicaciones que permitan establecer quién intervino y con qué finalidad.

Las grabaciones de experiencias inmersivas pueden contener información especialmente sensible porque registran conversaciones, reacciones corporales y espacios físicos. Su obtención debe respetar legalidad, necesidad y proporcionalidad. La utilidad investigativa no autoriza recopilar sesiones completas cuando solo una fracción resulta relevante. Deben aplicarse medidas de minimización, acceso restringido y protección de terceros. La difusión pública de la grabación puede causar un daño adicional a la víctima, por lo que la preservación probatoria debe diferenciarse claramente de la publicación o reproducción del contenido.

La evidencia generada por inteligencia artificial plantea riesgos particulares. Un archivo de voz, imagen o video puede ser sintético, modificado o combinado con material auténtico. La apariencia realista no permite presumir veracidad. El análisis debe examinar origen, historial de edición, herramienta utilizada y coherencia con otros registros. Varela et al. (2025) señalan que la inteligencia artificial aumenta la capacidad de producir contenidos fraudulentos y dificulta su detección. La autenticación debe apoyarse en múltiples elementos y no únicamente en observación visual.

Figura 11
Dificultades en la investigación de evidencia digital en el metaverso



Nota. La figura expone las principales dificultades para investigar evidencia digital en el metaverso, relacionadas con su atribución, autenticidad, volatilidad y fragmentación. Elaboración propia.

Santamaría et al. (2023) destacan que la custodia digital requiere identificar responsables, accesos y transferencias. Las plataformas cumplen una función decisiva porque controlan registros que el usuario no puede conservar directamente. Deben disponer de procedimientos para responder a solicitudes legítimas, preservar información y documentar su extracción. Sin embargo, no deberían entregar datos sin verificar autoridad, alcance y fundamento. La cooperación debe equilibrar investigación, privacidad y derechos de defensa. Una solicitud demasiado amplia puede exponer conversaciones y actividades ajenas al caso. La entrega debe limitarse a los registros pertinentes y realizarse mediante canales seguros que permitan comprobar su procedencia.

La jurisdicción determina qué autoridad puede investigar, juzgar y ejecutar una decisión. En el metaverso, el usuario, la víctima, la plataforma, el servidor y el resultado pueden encontrarse en países diferentes. La ubicación técnica de la infraestructura no siempre representa el vínculo más relevante. Kostenko et al. (2022) destacan que los entornos virtuales requieren criterios basados en efectos, residencia, actividad dirigida y relación sustancial con el territorio. La jurisdicción debe evitar tanto la ausencia de autoridad como la pretensión de que todos los Estados intervengan simultáneamente.

El lugar donde se produce el daño puede justificar la competencia cuando las consecuencias recaen sobre una persona situada en Ecuador. Sin embargo, la mera accesibilidad global de una plataforma no debería bastar para someterla a todas las

jurisdicciones. Debe examinarse si dirige servicios al país, acepta usuarios ecuatorianos, utiliza moneda local, realiza publicidad o mantiene una actividad económica significativa. Estos elementos ayudan a establecer una conexión razonable y previsible. La competencia no debe basarse únicamente en que el contenido pudiera visualizarse técnicamente desde el territorio.

Las cláusulas de elección de foro incluidas en términos de servicio pueden establecer tribunales o arbitrajes extranjeros. No obstante, su eficacia debe examinarse según la naturaleza de la relación y las normas imperativas aplicables. En contratos de consumo, una cláusula que obligue al usuario a litigar en un país lejano puede generar indefensión. La aceptación mediante un clic no elimina el control sobre cláusulas abusivas. La determinación jurisdiccional debe considerar acceso efectivo a la justicia, equilibrio contractual y protección de la parte más vulnerable.

La cooperación internacional puede ser necesaria para identificar usuarios, obtener registros, congelar activos o ejecutar decisiones. La rapidez resulta especialmente importante cuando la evidencia puede eliminarse o transferirse entre plataformas. Los mecanismos de asistencia deben permitir solicitudes específicas, autenticadas y proporcionales. La cooperación informal entre empresas puede facilitar una respuesta inicial, pero no sustituye los procedimientos legales cuando se requieren datos protegidos o medidas coercitivas. También deben respetarse las garantías de la persona investigada y la protección de información perteneciente a terceros.

La ley aplicable no siempre coincide con la jurisdicción. Un tribunal ecuatoriano podría conocer el caso y tener que determinar qué normativa regula un contrato, un daño o una transferencia. Los criterios pueden incluir residencia, lugar de cumplimiento, elección válida de las partes y país donde se producen los efectos principales. Kostenko et al. (2022) señalan que la pluralidad de conexiones jurídicas es una característica central de los mundos virtuales. La solución debe evitar que la arquitectura tecnológica permita seleccionar artificialmente la legislación menos protectora.

En materia penal, la competencia requiere examinar el lugar de ejecución, el resultado y los vínculos del responsable o de la víctima. Una conducta puede iniciarse desde otro país y producir una pérdida patrimonial o afectación personal en Ecuador. La investigación debe coordinar obtención de evidencia, identificación de cuentas y medidas sobre activos. No obstante, la extraterritorialidad no debe presumirse sin

fundamento legal. Cada actuación debe respetar soberanía, cooperación internacional y garantías procesales, especialmente cuando la evidencia se encuentra bajo control de una empresa extranjera.

La evidencia digital y la jurisdicción deben abordarse conjuntamente porque la autoridad competente necesita acceso legítimo a registros ubicados en diferentes sistemas y territorios. La preservación, integridad, metadatos y cadena de custodia determinan la confiabilidad de la prueba, mientras los criterios de conexión establecen quién puede solicitarla y valorarla. Alqahtany y Syed (2024) y Santamaría et al. (2023) respaldan la trazabilidad y documentación del manejo probatorio y permite contextualizar la dimensión jurisdiccional transfronteriza.

Capítulo 5

Gobernanza global y futuro de la regulación del metaverso

Rodolfo Marlon Mina Angulo



5.1 Soberanía y jurisdicción virtual

La expansión del metaverso desafía las categorías tradicionales de soberanía porque las actividades virtuales pueden desarrollarse simultáneamente en infraestructuras, plataformas y dispositivos ubicados en distintos países. Un usuario puede encontrarse físicamente en Ecuador, utilizar servidores extranjeros, contratar con una empresa domiciliada en otro Estado y relacionarse con personas de varias jurisdicciones. Esta dispersión no elimina la autoridad estatal, pero dificulta identificar qué ordenamiento resulta aplicable. Kostenko et al. (2022) destacan que los mundos virtuales requieren criterios jurídicos basados en conexiones sustanciales y no exclusivamente en la ubicación técnica de los servidores.

La soberanía continúa correspondiendo a los Estados y no a las plataformas digitales. Aunque una empresa establezca reglas internas, administre identidades o controle espacios virtuales, no adquiere potestad soberana equivalente a la estatal. Sus decisiones se fundamentan en contratos, propiedad tecnológica y organización privada. Las plataformas pueden moderar contenidos, suspender cuentas o definir condiciones de acceso, pero estas facultades permanecen sometidas a normas imperativas y control judicial. Kasiyanto y Kilinc (2022) advierten que la descentralización tecnológica no elimina la necesidad de autoridad jurídica ni convierte los protocolos en ordenamientos independientes.

La soberanía digital puede entenderse como la capacidad de un Estado para proteger derechos, exigir obligaciones y ejercer competencias respecto de actividades tecnológicas vinculadas con su territorio o población. Esta idea no implica controlar toda interacción transfronteriza, sino asegurar que las empresas que operan en el mercado nacional respeten la legislación aplicable. La Constitución de la República del Ecuador (2008) conserva plena relevancia frente a actividades virtuales cuando se afectan derechos de personas situadas en el país. La virtualidad del medio no reduce la obligación estatal de garantizar tutela efectiva.

La jurisdicción determina qué autoridad posee competencia para conocer una controversia, investigar una conducta o ejecutar una decisión. En el metaverso pueden coincidir varios criterios: domicilio de las partes, lugar del daño, ubicación de la empresa, sitio de cumplimiento contractual y país hacia el cual se dirige el servicio. Kostenko et al. (2022) sostienen que la pluralidad de conexiones exige evitar respuestas

automáticas. La ubicación de una cadena de bloques, por ejemplo, puede resultar indeterminada o irrelevante frente al lugar donde se producen los efectos principales.

El criterio territorial mantiene importancia cuando una conducta se ejecuta o produce consecuencias dentro de Ecuador. Una estafa realizada desde otro país puede ocasionar una pérdida patrimonial a un usuario ecuatoriano, mientras una filtración extranjera puede afectar datos tratados en el territorio nacional. Sin embargo, el lugar del resultado no debe utilizarse de manera ilimitada. La conexión debe ser real, previsible y jurídicamente significativa. De lo contrario, cualquier contenido accesible desde internet quedaría sometido simultáneamente a todas las jurisdicciones, generando inseguridad y conflictos de competencia.

El domicilio o residencia de las partes constituye otro criterio relevante. Una persona domiciliada en Ecuador puede reclamar protección frente a una plataforma extranjera cuando la relación se vincula de manera efectiva con el país. Al mismo tiempo, la nacionalidad por sí sola puede resultar insuficiente si toda la actividad se desarrolló en otro territorio. Kasiyanto y Kilinc (2022) señalan que la atribución de competencia debe considerar el conjunto de circunstancias. La residencia, el mercado objetivo y el lugar del daño suelen ofrecer conexiones más concretas que la nacionalidad aislada.

La actividad dirigida permite determinar si una plataforma extranjera orienta deliberadamente sus servicios hacia Ecuador. Pueden considerarse elementos como publicidad destinada al país, aceptación de usuarios ecuatorianos, uso de moneda local, atención en español, medios de pago nacionales o presencia comercial. La simple posibilidad de ingresar desde Ecuador no siempre basta. Kostenko et al. (2022) explican que la jurisdicción debe apoyarse en una vinculación razonablemente previsible para el proveedor. Este criterio protege al usuario sin imponer obligaciones universales por mera accesibilidad técnica.

Las cláusulas de elección de foro pueden aportar previsibilidad al indicar qué tribunales resolverán las controversias. No obstante, su validez depende de la naturaleza de la relación y del equilibrio entre las partes. En contratos de adhesión, una plataforma no debería obligar al consumidor a litigar exclusivamente en una jurisdicción remota cuando ello impide ejercer sus derechos. La Ley Orgánica de Defensa del Consumidor (2000) permite controlar cláusulas que generen indefensión. La autonomía contractual

no puede utilizarse para excluir normas imperativas ni vaciar el acceso efectivo a la justicia.

La elección de la ley aplicable tampoco resuelve todos los conflictos. Las partes pueden seleccionar un ordenamiento para regular determinadas obligaciones, pero esa elección no necesariamente desplaza normas obligatorias de consumo, datos, competencia o protección de menores. Kostenko et al. (2022) señalan que los mundos virtuales generan relaciones híbridas donde convergen contratos, derechos personales y actividades económicas. El juez debe distinguir qué materias pueden someterse a autonomía privada y cuáles permanecen vinculadas con intereses públicos que justifican la aplicación de la legislación nacional.

Figura 12
Desafíos de la soberanía y jurisdicción en el metaverso



Nota. La figura sintetiza los desafíos de soberanía y jurisdicción en el metaverso, considerando la autoridad estatal, la competencia legal, la ley aplicable y la elección del foro. Elaboración propia.

La ubicación de los datos puede influir en la investigación y ejecución de decisiones, aunque no determina por sí sola la jurisdicción sustantiva. Una plataforma puede almacenar registros en varios países o trasladarlos dinámicamente entre servidores. Basar toda competencia en el lugar técnico de almacenamiento generaría resultados inestables. La autoridad debe priorizar el vínculo entre la información, las partes y el hecho investigado. La localización de datos adquiere mayor relevancia para solicitudes

de preservación, acceso y cooperación que para definir automáticamente qué derecho regula la controversia.

Las arquitecturas descentralizadas dificultan la identificación de un operador único. Un protocolo puede funcionar mediante desarrolladores, validadores, interfaces, usuarios y organizaciones distribuidas. Sin embargo, la ausencia de una empresa central no significa ausencia de responsables. Kasiyanto y Kilinc (2022) sostienen que deben examinarse funciones, control y beneficios de cada actor. La jurisdicción puede vincularse con quienes desarrollan, administran interfaces, reciben ingresos o toman decisiones significativas. La descentralización técnica no debe utilizarse como mecanismo para escapar de toda obligación jurídica.

Las plataformas pueden ejercer una forma de regulación privada mediante códigos de conducta, sistemas de moderación y procedimientos internos. Estas normas pueden ordenar la convivencia, pero no sustituyen el derecho estatal. Una suspensión de cuenta puede ser válida contractualmente, mientras una sanción penal solo puede imponerse por una autoridad competente conforme al principio de legalidad. La soberanía exige mantener esta distinción. Los operadores administran servicios privados; los Estados garantizan derechos, resuelven controversias y aplican medidas coercitivas dentro de los límites establecidos por el ordenamiento.

Los conflictos positivos de jurisdicción aparecen cuando varios Estados consideran que poseen competencia sobre el mismo caso. Esto puede producir investigaciones paralelas, decisiones incompatibles o cargas excesivas para las partes. Los conflictos negativos surgen cuando ninguna autoridad acepta intervenir, dejando a la víctima sin protección. Kostenko et al. (2022) destacan la necesidad de criterios previsibles y coordinación internacional. La solución debe privilegiar la jurisdicción con conexión más estrecha, capacidad probatoria y posibilidad real de ejecutar la decisión, sin desconocer derechos fundamentales de las personas involucradas.

La ejecución de decisiones constituye una prueba concreta de la eficacia jurisdiccional. Un tribunal puede declarar una obligación, pero la medida será insuficiente si la plataforma, los activos o el responsable se encuentran fuera de su alcance. El reconocimiento de sentencias, la cooperación empresarial y los mecanismos internacionales permiten transformar una decisión formal en una reparación efectiva. Sin embargo, las plataformas no deberían ejecutar automáticamente órdenes extranjeras

sin verificar autenticidad, competencia y respeto de garantías. La colaboración debe someterse a procedimientos jurídicos claros y proporcionales.

La soberanía también exige proteger el orden público y los derechos fundamentales frente a modelos contractuales diseñados íntegramente por empresas extranjeras. Una plataforma que opera en Ecuador no debería desconocer normas nacionales mediante condiciones elaboradas en otra jurisdicción. Al mismo tiempo, el Estado debe evitar intervenciones desproporcionadas que fragmenten excesivamente el entorno digital. Kasiyanto y Kilinc (2022) plantean que la regulación debe equilibrar innovación, autonomía y protección. La respuesta adecuada requiere vínculos jurídicos claros y no una pretensión de control absoluto sobre toda actividad global.

En definitiva, la soberanía y la jurisdicción virtual deben construirse mediante criterios de conexión territorial, personal, contractual y económica. La ubicación de servidores, el domicilio de una empresa o la nacionalidad de un usuario no resuelven aisladamente la competencia. Kostenko et al. (2022) y Kasiyanto y Kilinc (2022) ofrecen fundamentos suficientes para analizar estos problemas sin recurrir artificialmente a fuentes sobre NFT, seguridad o consentimiento. La finalidad consiste en garantizar previsibilidad, acceso a la justicia y ejecución efectiva sin desconocer la naturaleza transfronteriza del metaverso.

5.2 Gobernanza de las plataformas

La gobernanza de las plataformas comprende el conjunto de reglas, órganos, procedimientos y decisiones mediante los cuales se administra un entorno virtual. Incluye la definición de condiciones de acceso, moderación, gestión de datos, seguridad, resolución de controversias y distribución de facultades entre usuarios y operadores. En el metaverso, esta gobernanza adquiere especial importancia porque las plataformas no solo alojan contenidos, sino que diseñan espacios, identidades y relaciones económicas. Su poder debe ejercerse mediante reglas previsibles, controles internos y mecanismos externos de supervisión.

Las plataformas desarrollan una forma de regulación privada al establecer términos de servicio, códigos de conducta y procedimientos de sanción. Estas normas pueden organizar la convivencia, pero no poseen la misma legitimidad ni fuerza que las leyes estatales. Una empresa puede suspender una cuenta o limitar determinadas funciones, pero no puede crear delitos ni imponer sanciones penales. Kostenko et al. (2022)

advierten que los entornos virtuales continúan vinculados con jurisdicciones y ordenamientos existentes. La gobernanza privada complementa la regulación estatal, pero no la sustituye.

El diseño tecnológico también forma parte de la gobernanza. La arquitectura determina quién puede acceder, comunicarse, transferir activos o moderar contenidos. Las decisiones incorporadas en el código pueden ser más efectivas que las reglas escritas, porque permiten o impiden conductas de manera inmediata. Munn y Weijers (2023) sostienen que el diseño distribuye poder y condiciona la autonomía dentro de los entornos virtuales. Una gobernanza responsable debe reconocer que cada configuración técnica produce efectos normativos y que esos efectos requieren justificación, evaluación y posibilidad de corrección.

La legitimidad de la gobernanza depende de que las reglas sean claras, accesibles y aplicadas de manera coherente. Los usuarios deben conocer qué conductas están prohibidas, qué medidas pueden imponerse y qué procedimiento existe para cuestionarlas. Las normas extensas, ambiguas o modificadas sin aviso reducen la previsibilidad. Una plataforma no debería depender exclusivamente de la aceptación formal de términos que pocos comprenden. La gobernanza requiere comunicación continua, resúmenes comprensibles y explicación de los cambios que afecten derechos, activos o participación.

La participación de los usuarios puede mejorar la calidad de las reglas y reducir decisiones desconectadas de la experiencia real. Las plataformas pueden crear consultas, consejos comunitarios, encuestas o mecanismos de propuesta. Sin embargo, la participación no debe ser meramente simbólica. Debe existir información suficiente sobre cómo se utilizarán las opiniones y qué decisiones permanecen bajo control empresarial. Jauhiainen et al. (2023) muestran que los entornos virtuales pueden fortalecer colaboración y comunidad, pero también reproducir concentraciones de poder si la participación carece de efectos reales.

La moderación constituye una de las funciones centrales de la gobernanza. Incluye prevención, detección y respuesta frente a acoso, fraude, violencia, desinformación o contenidos ilícitos. La plataforma debe diferenciar entre conductas dañinas y expresiones legítimas, considerando contexto, reiteración y gravedad. Chawki et al. (2024) advierte que los daños virtuales no pueden minimizarse, aunque tampoco deben

resolverse mediante sanciones automáticas e indiscriminadas. La gobernanza debe equilibrar seguridad, libertad de expresión, debido proceso y protección de las personas afectadas.

La transparencia de las decisiones fortalece la confianza. Las plataformas deberían publicar criterios de moderación, estadísticas sobre denuncias, tiempos de respuesta y resultados generales. Cheong (2024) vincula la transparencia con explicabilidad, participación y rendición de cuentas, especialmente cuando los sistemas automatizados condicionan el bienestar. Zhu et al. (2025) añade que la supervisión de plataformas requiere estrategias combinadas y participación de múltiples actores. La información debe permitir evaluar coherencia, proporcionalidad y posibles patrones discriminatorios sin revelar datos personales o secretos legítimos.

Tabla 14
Componentes esenciales de la gobernanza de plataformas virtuales

Componente	**Función principal**	**Riesgo de gobernanza**	**Medida recomendada**
Reglas de comunidad	Definir conductas permitidas	Ambigüedad o cambios inesperados	Normas claras y aviso previo
Moderación	Prevenir y sancionar abusos	Decisiones arbitrarias	Criterios públicos y revisión
Participación	Incorporar opiniones de usuarios	Consulta simbólica	Mecanismos con efectos verificables
Gestión de datos	Regular recopilación y uso	Vigilancia excesiva	Minimización y control del usuario
Seguridad	Proteger cuentas y sistemas	Medidas insuficientes	Gestión continua de riesgos
Sanciones	Responder a incumplimientos	Desproporción	Gradualidad y motivación
Apelación	Revisar decisiones	Falta de independencia	Instancia distinta y accesible
Transparencia	Informar políticas y resultados	Opacidad institucional	Reportes periódicos
Auditoría	Evaluar cumplimiento y sesgos	Autoevaluación limitada	Revisión externa
Reparación	Corregir daños y errores	Respuestas meramente formales	Restitución y seguimiento

Nota. La gobernanza efectiva requiere combinar reglas, diseño, participación, supervisión y mecanismos de reparación.

Los procedimientos sancionadores deben respetar garantías mínimas. Antes de imponer una medida grave, el usuario debería conocer la acusación, la regla aplicable y la evidencia esencial. También debe disponer de una oportunidad razonable para responder. Las medidas urgentes pueden aplicarse provisionalmente cuando exista riesgo inmediato, pero requieren revisión posterior. La gobernanza no puede depender de decisiones irreversibles adoptadas sin explicación. La proporcionalidad exige distinguir entre infracciones leves, conductas reiteradas y daños graves, evitando tratar todos los casos de la misma manera.

La apelación debe ser accesible, independiente y suficientemente rápida. No resulta adecuado que la misma herramienta automatizada revise su propia decisión sin intervención adicional. Cuando la sanción afecta trabajo, ingresos, activos o reputación, debe existir revisión humana competente. La plataforma debe informar plazos, criterios y resultado. Una apelación puramente formal no cumple su función si nunca permite modificar decisiones. La calidad de la gobernanza se demuestra también por su capacidad para reconocer errores, rectificar y restablecer los derechos afectados. Cheong (2024) vincula la rendición de cuentas con la posibilidad real de comprender, cuestionar y corregir decisiones que afectan el bienestar de las personas.

La protección de datos forma parte de la gobernanza porque las plataformas deciden qué información recopilan, con qué finalidad la utilizan y qué actores pueden acceder a ella. La LOPDP (2021) exige transparencia, finalidad, proporcionalidad y seguridad. Fernandez y Hui (2022) demuestran que la recopilación inmersiva incrementa los riesgos de vigilancia, reidentificación y exposición. Las decisiones sobre datos deben integrarse en estructuras de responsabilidad, supervisión, documentación y reparación, y no quedar reducidas a una política de privacidad aceptada al registrarse.

La seguridad también debe integrarse en la estructura de gobierno. Deben definirse responsables, protocolos de incidentes, mecanismos de auditoría y canales para reportar vulnerabilidades. Gupta et al. (2023) puede utilizarse para evaluar controles de confianza mínima, mientras Pooyandeh et al. (2022) aporta sobre riesgos técnicos. Sin embargo, estas fuentes no explican por sí solas la legitimidad institucional de las decisiones. La gobernanza exige conectar seguridad, responsabilidad y supervisión, evitando que los asuntos técnicos queden aislados de los derechos y obligaciones de los usuarios.

La gobernanza económica comprende reglas sobre comisiones, monedas internas, activos y acceso a mercados. Las plataformas pueden modificar precios, limitar transferencias o retirar bienes, afectando intereses patrimoniales. Estas decisiones deben ser previsibles, justificadas y sujetas a reclamación. Madanchian y Taherdoost (2024) destaca que la confianza y la sostenibilidad de los modelos económicos virtuales dependen de reglas comprensibles y de la continuidad razonable del ecosistema. En el ámbito económico, estas exigencias deben complementarse con transparencia contractual, equilibrio y protección del consumidor.

La descentralización introduce modelos de gobernanza basados en votaciones, tokens o comunidades distribuidas. Estos sistemas pueden ampliar la participación, aunque también concentrar poder en quienes poseen más recursos, conocimientos o activos. Kasiyanto y Kilinc (2022) señalan que la descentralización no garantiza automáticamente igualdad ni ausencia de responsables. Debe analizarse quién propone decisiones, quién controla el código y cómo se ejecutan los resultados. La apariencia comunitaria puede ocultar estructuras dominadas por desarrolladores, inversores o actores con capacidad económica superior.

La auditoría externa permite evaluar si la plataforma cumple sus reglas y la legislación aplicable. Puede abarcar moderación, seguridad, protección de datos, accesibilidad y decisiones automatizadas. En materia algorítmica, Papagiannidis et al. (2025) sitúan la auditoría dentro de las prácticas de gobernanza aplicables durante el ciclo de vida de la inteligencia artificial, mientras Zhu et al. (2025) destacan la necesidad de combinar participación de múltiples actores, supervisión pública y estrategias complementarias. Los hallazgos deben conducir a responsables, plazos y medidas verificables.

La reparación constituye un componente imprescindible. Cuando la plataforma aplica una sanción errónea, expone datos o permite la pérdida de activos, debe corregir las consecuencias. Puede ser necesario restituir cuentas, recuperar saldos, retirar información falsa o compensar daños. Una disculpa general no basta si persiste la afectación. La gobernanza responsable debe prever procedimientos de reparación desde el diseño y no improvisarlos después del incidente. También debe informar a la persona afectada sobre las medidas adoptadas y los mecanismos disponibles para continuar reclamando.

La supervisión pública resulta necesaria cuando las decisiones privadas afectan derechos fundamentales, mercados o servicios esenciales. El Estado no debe administrar directamente todas las plataformas, pero sí establecer límites, obligaciones de transparencia y mecanismos de control. Una regulación demasiado débil puede permitir abusos, mientras una intervención excesiva puede restringir innovación y libertad. La respuesta debe ser proporcional al tamaño, riesgo y poder de la plataforma. Las obligaciones más intensas deberían recaer sobre operadores con mayor capacidad de impacto y control.

La gobernanza de las plataformas requiere reglas claras, participación efectiva, moderación proporcional, transparencia, auditoría y reparación. No puede construirse mediante una acumulación artificial de fuentes sobre seguridad, NFT, identidad y consentimiento. Cada referencia debe utilizarse únicamente para el aspecto que realmente desarrolla. El marco general debe apoyarse en principios de legitimidad, debido proceso, rendición de cuentas y control público. Una plataforma bien gobernada no solo funciona técnicamente, sino que distribuye poder de manera justificable y permite cuestionar sus decisiones.

5.3 Modelos de regulación del metaverso

La regulación del metaverso no puede construirse mediante un único modelo uniforme, porque estos entornos integran relaciones contractuales, tratamiento de datos, actividades económicas, contenidos, propiedad intelectual y conductas potencialmente delictivas. Cada dimensión presenta riesgos y niveles de intervención diferentes. Un sistema excesivamente rígido puede limitar innovación y desarrollo tecnológico, mientras una regulación demasiado débil puede dejar a los usuarios sin protección efectiva. Zhu et al. (2025) sostienen que el carácter transfronterizo y complejo de los mundos virtuales exige combinar instrumentos públicos, privados y cooperativos.

El modelo de autorregulación se basa en normas creadas y aplicadas por las propias plataformas. Incluye términos de servicio, códigos comunitarios, políticas de privacidad y procedimientos internos de moderación. Su principal ventaja es la rapidez para adaptarse a cambios tecnológicos. Sin embargo, presenta riesgos de opacidad, concentración de poder y aplicación desigual. Kostenko et al. (2022) advierten que las reglas privadas no forman un ordenamiento soberano independiente. La autorregulación

puede complementar la ley, pero no sustituir garantías, controles externos ni obligaciones imperativas.

La corregulación combina normas estatales con estándares elaborados por empresas, asociaciones y organizaciones especializadas. El Estado define objetivos mínimos, mientras los actores tecnológicos desarrollan procedimientos técnicos para cumplirlos. Este modelo puede resultar útil cuando la regulación necesita actualizarse con rapidez. Sin embargo, requiere supervisión independiente y mecanismos para evitar que la industria diseñe reglas únicamente favorables a sus intereses. La participación privada debe aportar conocimiento técnico, pero las decisiones sobre derechos, sanciones y obligaciones esenciales deben conservar legitimidad pública y posibilidad de revisión.

La regulación basada en riesgos adapta las obligaciones a la probabilidad y gravedad de los daños. No todas las plataformas requieren los mismos controles. Un entorno utilizado por menores, que procesa datos biométricos o permite transacciones de alto valor presenta riesgos superiores a una experiencia limitada y sin monetización. Este modelo permite aplicar exigencias proporcionales sobre seguridad, auditoría, transparencia y supervisión. La dificultad consiste en definir categorías claras y evitar que las propias empresas minimicen artificialmente sus riesgos para quedar sometidas a obligaciones menos intensas.

La regulación sectorial aplica normas distintas según la actividad realizada dentro del metaverso. Las operaciones financieras pueden someterse a reglas económicas, los datos personales a legislación de privacidad y los contenidos protegidos a propiedad intelectual. Este enfoque aprovecha instituciones existentes y evita crear un régimen completamente separado. Kostenko et al. (2022) sostienen que muchas controversias virtuales pueden resolverse mediante categorías jurídicas vigentes. Sin embargo, la fragmentación puede producir vacíos cuando una misma conducta combina simultáneamente varias materias.

El modelo integral propone una ley específica que organice principios, definiciones y responsabilidades aplicables a todo el metaverso. Su ventaja consiste en ofrecer coherencia y visibilidad normativa. No obstante, una legislación demasiado detallada puede quedar rápidamente desactualizada o intentar regular tecnologías todavía inestables. La utilidad de una norma integral depende de que se concentre en principios duraderos, como transparencia, seguridad, protección de derechos y cooperación,

dejando aspectos técnicos a reglamentos o estándares capaces de adaptarse con mayor rapidez.

La regulación por diseño busca incorporar obligaciones directamente en la arquitectura tecnológica mediante privacidad predeterminada, límites de contacto, confirmaciones de pago y controles de seguridad. Munn y Weijers (2023) muestran que la arquitectura influye directamente en la autonomía y el bienestar de los participantes, mientras Zhu et al. (2025) señalan que la regulación de plataformas dinámicas requiere combinar autonomía empresarial, supervisión pública y participación de múltiples actores. Las medidas técnicas deben permanecer transparentes, proporcionales, auditables y sujetas a corrección.

Tabla 15
Principales modelos de regulación aplicables al metaverso

Modelo	Característica central	Ventaja principal	Riesgo predominante
Autorregulación	Reglas creadas por plataformas	Adaptación rápida	Falta de control externo
Correlación	Coordinación entre Estado e industria	Integración de conocimiento técnico	Captura regulatoria
Basado en riesgos	Obligaciones proporcionales al peligro	Flexibilidad	Subestimación de riesgos
Sectorial	Aplicación de normas por materia	Uso de marcos existentes	Fragmentación institucional
Integral	Ley específica para el metaverso	Coherencia general	Obsolescencia normativa
Regulación por diseño	Obligaciones incorporadas en la arquitectura	Prevención temprana	Restricciones automáticas excesivas
Experimental	Pruebas controladas y supervisadas	Innovación regulada	Protección insuficiente durante el ensayo
Internacional coordinado	Estándares y cooperación entre Estados	Reducción de conflictos	Dificultad de consenso
Comunitario	Participación directa de usuarios	Mayor legitimidad social	Dominio de grupos organizados
Híbrido	Combinación de varios modelos	Adaptación a diferentes riesgos	Complejidad de implementación

Nota. Ningún modelo resulta suficiente por sí solo; la regulación efectiva requiere una combinación proporcional de instrumentos.

Los espacios regulatorios experimentales permiten probar tecnologías y modelos de negocio bajo supervisión temporal. Las empresas pueden desarrollar servicios innovadores mientras las autoridades observan riesgos, recopilan evidencia y ajustan requisitos. Este modelo puede ser útil para contratos inteligentes, activos digitales o experiencias biométricas. Sin embargo, la experimentación no debe convertirse en una zona sin derechos. Los participantes deben recibir información clara, protección frente a daños y vías de reclamación. La flexibilización normativa debe limitarse a aspectos concretos y durante periodos definidos.

La regulación de los activos digitales requiere un enfoque diferenciado según su función económica. Los tokens pueden representar acceso, utilidad, colección, credenciales o expectativas de rendimiento, y cada modalidad genera riesgos distintos. Martínez et al. (2024) permiten separar el registro técnico, el archivo y los derechos asociados, mientras Madanchian y Taherdoost (2024) explica la relevancia de la confianza y la sostenibilidad del modelo de negocio. La respuesta regulatoria debe construirse a partir de la función ofrecida, la información comercial, la transferibilidad y la exposición económica del usuario, sin extender conclusiones propias de los NFT a todos los activos virtuales.

La regulación internacional coordinada busca reducir conflictos entre Estados y establecer estándares mínimos sobre identidad, seguridad, protección de datos y cooperación. Kostenko et al. (2022) consideran que las actividades transfronterizas requieren criterios comunes de conexión y responsabilidad. Sin embargo, la armonización completa puede resultar difícil por diferencias culturales, constitucionales y económicas. Un modelo realista debe concentrarse en principios compartidos y mecanismos de reconocimiento, permitiendo que cada Estado mantenga márgenes para proteger derechos y aplicar normas acordes con su ordenamiento.

La participación comunitaria puede incorporarse mediante consultas, consejos de usuarios, votaciones y procedimientos colaborativos. Este modelo busca legitimar decisiones que afectan directamente la experiencia virtual. No obstante, la participación debe diseñarse para evitar que grupos con mayor conocimiento, tiempo o recursos controlen el proceso. Jauhiainen et al. (2023) muestran que las comunidades virtuales pueden fomentar colaboración, aunque también reproducir desigualdades. Las

decisiones fundamentales sobre derechos no deberían depender exclusivamente de mayorías internas ni de la posesión de tokens.

El modelo de regulación adaptativa utiliza revisión periódica, indicadores y evaluaciones de impacto para modificar obligaciones según la evolución tecnológica. En lugar de establecer reglas definitivas, crea ciclos de seguimiento y corrección. Esta estrategia puede responder mejor a cambios en dispositivos, inteligencia artificial y prácticas de mercado. Sin embargo, la flexibilidad no debe generar incertidumbre permanente. Los principios básicos y las garantías mínimas deben mantenerse estables, mientras los aspectos técnicos pueden actualizarse mediante reglamentos, estándares o lineamientos sometidos a consulta y control.

La supervisión basada en transparencia exige a las plataformas publicar información sobre riesgos, moderación, decisiones automatizadas, incidentes y modelos económicos. Esta información permite que autoridades, investigadores y usuarios evalúen su funcionamiento. No obstante, la transparencia por sí sola no corrige abusos. Los reportes deben ser verificables, comparables y acompañados de consecuencias cuando revelen incumplimientos. Una regulación eficaz no puede limitarse a exigir documentos extensos que pocas personas comprenden. Debe combinar información accesible, auditoría y capacidad real de intervención.

El modelo sancionador actúa después del incumplimiento mediante multas, reparación, suspensión o responsabilidad. Su función es necesaria para garantizar que las obligaciones tengan consecuencias. Sin embargo, una regulación basada únicamente en sanciones resulta insuficiente frente a daños difíciles de revertir. La prevención, el diseño seguro y la supervisión temprana deben acompañar la respuesta posterior. Las sanciones también deben ser proporcionales al tamaño, beneficio y gravedad de la conducta, evitando que las multas se conviertan en costos ordinarios para plataformas con gran capacidad económica.

Para Ecuador, un modelo híbrido podría combinar legislación general, regulación sectorial y obligaciones basadas en riesgos. Las normas vigentes sobre consumo, datos, contratación y responsabilidad pueden aplicarse a numerosas actividades, mientras disposiciones específicas podrían cubrir transparencia de plataformas, activos virtuales y entornos inmersivos de alto riesgo. No sería necesario crear una autoridad completamente nueva si se coordinan las instituciones existentes. La prioridad debería

ser definir competencias, procedimientos y estándares comunes que eviten duplicaciones, vacíos y respuestas contradictorias.

La elección del modelo regulatorio debe considerar capacidad institucional, nivel de desarrollo tecnológico y protección efectiva de derechos. Importar marcos extranjeros sin adaptación puede generar normas difíciles de aplicar. Kostenko et al. (2022) destacan que la regulación debe atender a las conexiones jurídicas y capacidades institucionales reales. Ecuador necesita instrumentos comprensibles, fiscalizables y compatibles con su Constitución. La innovación debe promoverse mediante reglas previsibles, pero no mediante excepciones amplias que trasladen los riesgos a usuarios, consumidores o personas vulnerables.

La regulación del metaverso requiere una combinación de autorregulación, corregulación, normas sectoriales, diseño preventivo y supervisión pública. Kostenko et al. (2022) permiten situar estas herramientas dentro de los ordenamientos existentes, mientras Zhu et al. (2025) destacan la necesidad de capacidades públicas frente a sistemas opacos y redes complejas. El modelo más adecuado será aquel que combine flexibilidad tecnológica con garantías jurídicas estables, participación de los afectados y mecanismos verificables de rendición de cuentas.

5.4 Cooperación jurídica internacional

La cooperación jurídica internacional resulta indispensable cuando una conducta desarrollada en el metaverso involucra usuarios, plataformas, datos, activos o infraestructuras situados en diferentes países. En estos casos, una autoridad nacional puede carecer de acceso directo a registros, responsables o bienes necesarios para investigar y reparar el daño. La cooperación permite superar esas limitaciones mediante asistencia entre autoridades, preservación de información y reconocimiento de decisiones. Kostenko et al. (2022) destacan que la dimensión transfronteriza de los mundos virtuales exige mecanismos coordinados capaces de responder con rapidez y seguridad jurídica.

La cooperación jurídica no debe limitarse a solicitudes judiciales emitidas después de que la evidencia haya desaparecido. Los entornos virtuales requieren mecanismos previos de contacto entre autoridades, procedimientos urgentes de preservación, identificación de representantes de las plataformas y reglas para reconocer y ejecutar decisiones extranjeras. También deben diferenciarse la conservación provisional de

información, su entrega formal y su utilización probatoria, pues cada fase exige una base jurídica y garantías distintas. La rapidez tecnológica no justifica omitir el debido proceso, pero obliga a diseñar vías capaces de impedir que cuentas, registros o activos sean eliminados mientras se tramita la asistencia internacional.

La Conferencia de La Haya de Derecho Internacional Privado (2024) ha señalado que las controversias de la economía digital involucran problemas de jurisdicción, ley aplicable, reconocimiento de decisiones y relaciones entre plataformas y usuarios. Estas cuestiones adquieren mayor complejidad cuando existen contratos de consumo, infracciones ubicuas, activos digitales o estructuras descentralizadas. Para Ecuador, la cooperación futura debería priorizar solicitudes electrónicas normalizadas, autoridades de contacto, preservación urgente de evidencia y coordinación con proveedores extranjeros, manteniendo criterios de necesidad, proporcionalidad, autenticidad y protección de terceros.

La asistencia jurídica internacional comprende solicitudes formales destinadas a obtener pruebas, localizar personas, ejecutar diligencias o asegurar activos. Su eficacia depende de que la autoridad requirente identifique claramente el hecho, la información buscada y su relevancia para el procedimiento. Las solicitudes excesivamente amplias pueden retrasarse o rechazarse por afectar derechos de terceros. Deben delimitar cuentas, periodos, transacciones y categorías de datos. La precisión facilita la cooperación y reduce el riesgo de recopilar información ajena a la investigación o desproporcionada respecto del objetivo perseguido.

La preservación urgente de datos constituye una de las medidas más importantes porque los registros digitales pueden eliminarse, sobrescribirse o trasladarse en poco tiempo. Una plataforma puede conservar historiales durante periodos limitados, mientras una cuenta comprometida puede modificar información antes de que exista una orden formal. Chow et al. (2023) señalan que las arquitecturas distribuidas complican la retención y localización de registros. La cooperación debe permitir solicitudes tempranas de conservación, diferenciándolas de la entrega definitiva, que requerirá cumplir los procedimientos y garantías correspondientes.

La preservación no debe convertirse en vigilancia general. La solicitud debe indicar qué datos se conservarán, durante cuánto tiempo y con qué relación respecto del incidente. Puede comprender accesos, mensajes, transacciones, archivos o registros de

moderación vinculados con una cuenta o periodo determinado. La plataforma debe mantener la integridad de la información y documentar cualquier intervención. Al mismo tiempo, debe evitar conservar de manera indiscriminada conversaciones, movimientos o actividades de personas no relacionadas con el caso, protegiendo privacidad y confidencialidad.

La identificación de responsables puede requerir combinar información de varias entidades. Una dirección digital puede estar vinculada con una plataforma de intercambio, una cuenta con un proveedor de correo y un acceso con un dispositivo situado en otro país. Fiaz et al. (2024) explican que la atribución de conductas informáticas exige relacionar registros técnicos con identidad y contexto. La cooperación debe permitir reconstruir esa cadena sin presumir que el titular formal de una cuenta fue necesariamente quien ejecutó la acción investigada.

Las plataformas privadas desempeñan una función relevante porque controlan datos que no siempre se encuentran disponibles para las autoridades. Deben contar con procedimientos para recibir solicitudes legítimas, verificar su autenticidad y responder dentro de plazos razonables. Sin embargo, su cooperación no puede depender exclusivamente de políticas voluntarias o relaciones informales. Es necesario establecer criterios legales sobre conservación, entrega, confidencialidad y notificación. La empresa debe proteger la investigación sin convertirse en una autoridad que decida por sí sola sobre culpabilidad o responsabilidad jurídica.

Santamaría et al. (2023) subrayan que la transferencia de evidencia debe conservar integridad, trazabilidad y registro de cada interviniente. La transferencia internacional de evidencia requiere garantizar autenticidad, integridad y trazabilidad. Los registros enviados desde otro país deben acompañarse de información sobre su origen, método de extracción y condiciones de conservación. Las copias digitales pueden verificarse mediante resúmenes criptográficos, sellos de tiempo y documentación de cadena de custodia. Una evidencia técnicamente válida puede perder fuerza si no se conoce quién la obtuvo o si fue modificada durante su traslado. La cooperación debe utilizar canales seguros y formatos que permitan revisar posteriormente la información.

La localización de activos digitales puede requerir el análisis de cadenas de bloques, plataformas de intercambio y servicios de custodia. La trazabilidad técnica permite seguir movimientos, pero no siempre identificar a la persona que controla una dirección.

Kostenko et al. (2022) advierten que el registro distribuido no sustituye la atribución jurídica. Para congelar o recuperar activos se necesita vincular transacciones con usuarios, comprobar la naturaleza del bien y obtener la colaboración de operadores capaces de suspender transferencias o identificar a sus clientes.

Las medidas provisionales pueden ser necesarias cuando existe riesgo de pérdida de evidencia, fuga de activos o continuidad del daño. Entre ellas se encuentran la preservación de cuentas, el congelamiento temporal de fondos y la suspensión de contenidos específicos. Estas decisiones deben ser adoptadas por autoridades competentes o ejecutadas conforme a solicitudes legítimas. Su duración debe ser limitada y revisable. La urgencia no elimina el derecho de defensa ni permite mantener indefinidamente restricciones que fueron impuestas antes de determinar la responsabilidad.

La ejecución internacional de decisiones constituye una fase diferente de la investigación. Una sentencia que ordena indemnización, restitución de activos o retiro de contenido puede requerir reconocimiento en el país donde se encuentra el responsable o la plataforma. La cooperación debe permitir verificar competencia, firmeza y compatibilidad con el orden público. No toda decisión extranjera puede ejecutarse automáticamente. Sin embargo, la ausencia de mecanismos ágiles puede convertir la tutela judicial en una declaración sin efectos prácticos frente a operadores situados fuera del territorio nacional.

Figura 13
Mecanismo de cooperación jurídica internacional



Nota. Se presentan mecanismos de cooperación jurídica internacional para proteger evidencia y ejecutar decisiones. Elaboración propia.

La protección de víctimas exige respuestas rápidas cuando el daño continúa circulando entre plataformas o jurisdicciones. Una identidad suplantada, un contenido íntimo o una amenaza puede replicarse antes de completar los procedimientos ordinarios. Chawki et

al. (2024) destaca que la persistencia digital puede ampliar considerablemente las consecuencias. La cooperación debería facilitar canales de emergencia para retirar temporalmente contenido, preservar evidencia y proteger cuentas, sin sustituir la revisión jurídica posterior. La medida inicial debe ser específica, documentada y susceptible de control.

Los equipos conjuntos de investigación pueden resultar útiles frente a fraudes organizados, ataques informáticos o redes que operan mediante múltiples plataformas. Estos mecanismos permiten compartir información, coordinar diligencias y evitar duplicación de esfuerzos. Varela et al. (2025) señalan que la inteligencia artificial y la automatización aumentan la escala de la ciberdelincuencia. La cooperación debe asignar funciones claras, determinar qué autoridad conserva la dirección del caso y establecer reglas sobre uso, almacenamiento y transferencia de la información obtenida.

El intercambio internacional de alertas de ciberseguridad puede prevenir que una vulnerabilidad o modalidad de fraude afecte repetidamente a usuarios de distintos países. Pooyandeh et al. (2022) destacan que los ataques pueden propagarse entre dispositivos, cuentas y servicios conectados. Las autoridades y empresas pueden compartir indicadores técnicos, patrones de acceso y métodos utilizados. Sin embargo, estos intercambios deben minimizar datos personales y evitar listas opacas que produzcan bloqueos automáticos. La prevención debe diferenciar información técnica de acusaciones sobre personas concretas.

La doble incriminación puede influir en la asistencia penal cuando la conducta investigada debe ser delictiva tanto en el Estado requirente como en el requerido. Las diferencias normativas pueden dificultar la cooperación frente a conductas virtuales novedosas. No todos los países tipifican de igual manera el acceso ilícito, la suplantación o determinadas formas de violencia digital. La solicitud debe describir los hechos y no depender exclusivamente del nombre local del delito. Esto permite identificar equivalencias sustanciales entre figuras jurídicas y evitar rechazos basados únicamente en diferencias terminológicas.

La protección de datos debe mantenerse durante toda la cooperación. La transferencia internacional de información requiere una base jurídica, medidas de seguridad y limitación de finalidad. Los datos recibidos para investigar un fraude no deberían utilizarse posteriormente para objetivos incompatibles. También deben establecerse

plazos de conservación y procedimientos de eliminación cuando la información deje de ser necesaria. La cooperación eficaz no exige debilitar la privacidad, sino crear mecanismos que permitan obtener evidencia pertinente sin recopilar o reutilizar datos de manera indiscriminada.

Ecuador necesita fortalecer canales institucionales para responder a solicitudes relacionadas con plataformas, activos digitales y evidencia inmersiva. Esto incluye capacitación técnica, puntos de contacto especializados y protocolos entre autoridades judiciales, fiscales, policiales y organismos de protección de datos. No resulta necesario repetir en este apartado todas las reglas territoriales de la LOPDP (2021) o del COIP (2014). La prioridad consiste en convertir las competencias existentes en procedimientos operativos que permitan preservar registros, identificar responsables y ejecutar decisiones dentro de plazos compatibles con la velocidad tecnológica.

La cooperación jurídica internacional debe concentrarse en asistencia, preservación, identificación, transferencia de evidencia y ejecución de decisiones. Su eficacia depende de solicitudes específicas, canales seguros y garantías de proporcionalidad. Los problemas de jurisdicción explican la necesidad de coordinación entre Estados, mientras la conservación y autenticidad de los registros requieren protocolos forenses compatibles. La respuesta internacional debe evitar tanto la impunidad derivada de la fragmentación territorial como la recopilación indiscriminada de información ajena al caso investigado (Kostenko et al., 2022; Alqahtany y Syed, 2024).

5.5 Derechos humanos y diseño tecnológico

Los derechos humanos deben constituir un criterio central en el diseño del metaverso, porque las decisiones técnicas condicionan la forma en que las personas participan, se expresan, se relacionan y protegen su identidad. La arquitectura de una plataforma puede facilitar autonomía y seguridad, pero también permitir vigilancia, discriminación o exclusión. El respeto de derechos no debe limitarse a declaraciones generales incluidas en las condiciones de uso. Debe reflejarse en configuraciones, permisos, mecanismos de control y procedimientos capaces de prevenir y corregir afectaciones concretas (Munn y Weijers, 2023).

El diseño tecnológico no es neutral, pues distribuye capacidades entre usuarios, desarrolladores y operadores. La ubicación de botones, los permisos predeterminados, la visibilidad de las denuncias y la forma de presentar opciones influyen en las

decisiones individuales. Munn y Weijers (2023) sostienen que estas elecciones pueden fortalecer o reducir la autonomía. Una plataforma respetuosa de los derechos humanos debe evitar estructuras que conduzcan al usuario hacia conductas no deseadas, dificulten el rechazo o conviertan la participación en una aceptación tácita de vigilancia y explotación económica.

La dignidad humana exige que las personas no sean tratadas únicamente como fuentes de datos, atención o ingresos. Los usuarios construyen identidades, relaciones y proyectos dentro de los entornos virtuales, por lo que las decisiones tecnológicas pueden afectar dimensiones relevantes de su personalidad. Castillo et al. (2024) destacan que la identidad digital se integra mediante atributos visuales, conductuales y sociales. La plataforma debe impedir apropiaciones indebidas, manipulación degradante y usos que reduzcan al usuario a un perfil comercial sin control sobre su representación.

La autonomía requiere que las personas puedan tomar decisiones informadas y modificar sus preferencias durante la experiencia. El consentimiento no debe considerarse definitivo por haberse aceptado al ingresar a la plataforma. Sakka et al. (2026) señalan que los límites digitales deben poder establecerse, retirarse y ajustarse en tiempo real. Esto resulta especialmente importante en interacciones sociales, contacto entre avatares y uso de dispositivos hápticos. El diseño debe permitir detener experiencias, bloquear usuarios y desactivar funciones sin imponer recorridos complejos o consecuencias desproporcionadas.

La privacidad debe incorporarse desde el diseño porque los dispositivos inmersivos recopilan voz, mirada, movimientos, ubicación y respuestas corporales. Sorrentino y López (2025) advierten que estos datos permiten inferir características que la persona no ha comunicado expresamente. Las configuraciones predeterminadas deberían limitar la recopilación a lo necesario para cada función. También deben ofrecer controles comprensibles sobre almacenamiento, uso y transferencia. La posibilidad técnica de observar al usuario con gran precisión no convierte esa vigilancia en jurídicamente legítima ni funcionalmente indispensable.

La libertad de expresión también depende de la arquitectura. Una plataforma puede ampliar oportunidades de creación, reunión y participación, pero sus sistemas de moderación pueden restringir contenidos de manera opaca. Peña y Rubio (2024)

resaltan el potencial educativo y comunicativo de los entornos inmersivos cuando facilitan interacción significativa. Sin embargo, la moderación debe distinguir entre protección frente al daño y eliminación de expresiones controvertidas. Las restricciones necesitan reglas claras, motivación suficiente y procedimientos de revisión cuando afectan la participación del usuario.

La igualdad y la no discriminación requieren analizar cómo el diseño trata diferentes cuerpos, identidades, idiomas y capacidades. Un sistema de reconocimiento puede funcionar peor con determinados tonos de voz, movimientos o características físicas. También puede excluir a quienes no utilizan dispositivos de última generación. La discriminación no siempre surge de una intención explícita, sino de datos incompletos, estándares limitados o decisiones comerciales. La plataforma debe evaluar impactos, consultar a grupos diversos y corregir barreras que produzcan desventajas sistemáticas en acceso o participación.

Tabla 16
Derechos humanos y exigencias de diseño en el metaverso

Derecho o principio	Riesgo de diseño	Exigencia tecnológica	Mecanismo de garantía
Dignidad	Tratamiento del usuario como objeto de explotación	Límites al uso de identidad y conducta	Políticas claras y control individual
Autonomía	Opciones manipuladoras o difíciles de rechazar	Decisiones reversibles	Consentimiento granular
Privacidad	Recopilación continua de datos corporales	Minimización por defecto	Paneles de control accesibles
Libertad de expresión	Moderación automática excesiva	Evaluación contextual	Apelación y revisión humana
Igualdad	Sesgos en reconocimiento y acceso	Pruebas con poblaciones diversas	Auditorías de impacto
Integridad personal	Contactos o estímulos no consentidos	Límites espaciales y hápticos	Bloqueo inmediato
Identidad	Copia o manipulación de avatares	Verificación proporcional	Denuncia y retirada
Accesibilidad	Interfaces incompatibles con discapacidad	Diseño universal	Tecnologías de asistencia
Participación	Reglas impuestas sin consulta	Herramientas colaborativas	Procesos inclusivos

Derecho o principio	Riesgo de diseño	Exigencia tecnológica	Mecanismo de garantía
Seguridad	Exposición a ataques o suplantación	Protección desde el diseño	Autenticación y respuesta

Nota. La protección efectiva exige traducir cada derecho en funciones, restricciones y procedimientos verificables.

La integridad personal puede verse afectada cuando el diseño permite aproximaciones invasivas, estímulos hápticos o persecución persistente. Sakka et al. (2026) destacan que los límites deben expresarse de forma clara y modificarse durante la interacción. Las zonas personales, la desactivación inmediata de contacto y los bloqueos entre cuentas son medidas relevantes. Sin embargo, estas funciones deben estar activadas por defecto cuando el riesgo sea elevado. No resulta adecuado exigir que la víctima configure anticipadamente todas las formas posibles de protección frente a conductas abusivas.

La identidad digital necesita protección tanto frente a terceros como frente a la propia plataforma. Un avatar puede reflejar rasgos personales, culturales, profesionales o afectivos que forman parte de la presentación social del usuario. Castillo et al. (2024) señalan que la identidad digital combina autenticación, representación y reconocimiento. El diseño debe facilitar la denuncia de copias, permitir demostrar titularidad y evitar modificaciones no autorizadas. También debe informar cuándo una representación es sintética, promocional o controlada por un sistema automatizado.

La accesibilidad constituye una condición para el ejercicio efectivo de derechos. Una plataforma técnicamente disponible puede ser inaccesible para personas con discapacidad visual, auditiva, motora o cognitiva. Peña y Rubio (2024) destacan que la utilidad educativa de los entornos inmersivos depende de la adaptación de recursos y metodologías. El diseño debe incorporar subtítulos, alternativas sonoras, ajustes de movimiento, compatibilidad con tecnologías de asistencia y opciones de navegación simplificada. La accesibilidad no debe ofrecerse como complemento opcional, sino como componente básico del servicio.

La seguridad desde el diseño protege derechos cuando reduce riesgos de suplantación, vigilancia, apropiación de cuentas y pérdida de activos. Gupta et al. (2023) desarrollan un modelo de confianza cero basado en verificación continua, segmentación y control contextual de accesos. Estas medidas deben aplicarse de forma proporcional, evitando que la seguridad justifique vigilancia permanente o identificación biométrica

obligatoria. Su legitimidad depende de la finalidad, el riesgo, la minimización de datos y la existencia de alternativas menos invasivas.

La protección de menores requiere configuraciones especiales porque poseen menor capacidad para comprender riesgos y consecuencias. Las plataformas deben limitar contactos privados, publicidad personalizada, compras impulsivas y recopilación de datos. También deben utilizar lenguaje apropiado para la edad y permitir intervención de representantes sin convertir la experiencia en vigilancia familiar absoluta. El interés superior del menor exige diseños que reduzcan exposición y manipulación. No basta con trasladar la responsabilidad a los padres cuando la empresa controla las funciones, incentivos y mecanismos de interacción.

La participación de los usuarios puede mejorar la legitimidad del diseño. Las comunidades deben intervenir en pruebas, consultas y evaluación de nuevas funciones, especialmente cuando afectan privacidad, accesibilidad o moderación. Peña y Rubio (2024) muestran que la participación fortalece experiencias educativas y colaborativas. Sin embargo, la consulta debe incluir grupos habitualmente excluidos y no limitarse a usuarios con mayor actividad o poder económico. El diseño participativo permite identificar daños que los desarrolladores podrían no prever desde su propia experiencia social y tecnológica.

La evaluación de impacto en derechos humanos permite anticipar consecuencias antes de implementar una función. Debe analizar finalidad, población afectada, riesgos previsibles, medidas de reducción y alternativas menos restrictivas. Una evaluación no debe convertirse en un documento interno sin efectos. Sus resultados deben influir en el diseño, establecer responsables y generar revisiones posteriores. Cuando la función involucra biometría, menores, moderación automatizada o contacto háptico, la evaluación debe ser más rigurosa y contar con participación interdisciplinaria y mecanismos externos de supervisión.

La reparación también debe formar parte del diseño. Las plataformas deben prever cómo recuperar cuentas, eliminar copias de avatares, revisar sanciones y detener interacciones abusivas. Una arquitectura que solo permite imponer medidas, pero no corregir errores, genera indefensión. Sorrentino y López (2025) advierten que los daños relacionados con identidad y privacidad pueden persistir mediante datos derivados y perfiles. La reparación debe abarcar no solo el contenido visible, sino también registros,

clasificaciones y decisiones automatizadas que continúen produciendo efectos sobre el usuario.

Los derechos humanos deben traducirse en decisiones tecnológicas concretas sobre privacidad, identidad, accesibilidad, seguridad, consentimiento y participación. Cheong (2024) permite examinar la transparencia, la explicabilidad y la rendición de cuentas de los sistemas automatizados; Sakka et al. (2026) respaldan la incorporación de límites y consentimiento durante la interacción; y Berrezueta et al. (2025) aportan criterios específicos de accesibilidad para personas sordas. Estas perspectivas deben integrarse sin convertir una sola fuente especializada en fundamento general de todos los derechos involucrados.

5.6 Transparencia y responsabilidad algorítmica

La transparencia algorítmica constituye una condición esencial para que las decisiones automatizadas utilizadas en el metaverso puedan ser comprendidas, evaluadas y cuestionadas. Las plataformas emplean algoritmos para recomendar contenidos, moderar conductas, personalizar experiencias, asignar visibilidad, detectar fraude y restringir cuentas. Estas decisiones pueden afectar participación, reputación, privacidad o patrimonio. No basta con informar que existe inteligencia artificial. El usuario debe conocer qué función cumple el sistema, qué información utiliza y qué consecuencias relevantes puede producir sobre sus derechos.

La transparencia no exige necesariamente publicar el código fuente completo ni revelar secretos empresariales. Küsters (2026) muestra que, en agentes de inteligencia artificial del metaverso, la información sobre identidad automatizada, finalidad y capacidad de influencia es indispensable para evitar una confianza injustificada. Su finalidad consiste en proporcionar información significativa sobre objetivos, criterios generales, datos utilizados y efectos previsibles. Una explicación puramente técnica puede resultar inútil para la mayoría de usuarios, mientras una descripción demasiado general impide comprender la decisión. La información debe adaptarse al destinatario y al nivel de impacto. Cuanto más grave sea la consecuencia, mayor debe ser la precisión y profundidad de la explicación ofrecida por la plataforma.

La explicabilidad se refiere a la capacidad de comunicar por qué un sistema produjo un resultado determinado. En el metaverso puede ser necesaria cuando una cuenta es suspendida, una transacción se bloquea o un usuario recibe una clasificación de riesgo.

Cheong (2024) sostiene que la explicación debe integrarse con mecanismos de participación y responsabilidad, no limitarse a una descripción técnica. La plataforma debe identificar factores principales, permitir detectar errores y ofrecer una vía de revisión capaz de modificar efectivamente el resultado.

La LOPDP (2021), artículo 20, reconoce garantías relacionadas con decisiones basadas únicamente en valoraciones automatizadas que produzcan efectos jurídicos o significativos. Este marco resulta aplicable cuando la plataforma clasifica perfiles, restringe funciones o adopta medidas relevantes sin intervención humana suficiente. El usuario debe recibir información sobre la lógica aplicada y contar con mecanismos para expresar su posición. La automatización puede mejorar rapidez y consistencia, pero no debe eliminar la posibilidad de revisión cuando la decisión afecta de manera sustancial sus intereses.

La responsabilidad algorítmica exige identificar qué personas u organizaciones diseñan, implementan y supervisan el sistema. Un algoritmo no constituye un sujeto jurídico autónomo capaz de responder por los daños que genera. La responsabilidad debe recaer sobre quienes seleccionan datos, establecen objetivos, aprueban su uso o mantienen el sistema en funcionamiento. La complejidad tecnológica no puede convertirse en una excusa para afirmar que nadie controla el resultado. Deben existir funciones claramente asignadas, documentación y capacidad institucional para corregir fallos.

La calidad de los datos influye directamente en la confiabilidad de las decisiones. Información incorrecta, incompleta o desactualizada puede generar suspensiones, recomendaciones o perfiles equivocados. También puede ocurrir que datos obtenidos en un contexto sean utilizados para finalidades diferentes. La plataforma debe verificar pertinencia, exactitud y representatividad antes de emplearlos. Cheong (2024) señala que la transparencia y la rendición de cuentas requieren explicar qué información sustenta una decisión y ofrecer mecanismos para cuestionar resultados perjudiciales.

Cheong (2024) destaca que la rendición de cuentas exige evaluar discriminación, bienestar y efectos distributivos. El sesgo algorítmico puede producir resultados desiguales cuando los datos o criterios reflejan prejuicios previos. Un sistema de reconocimiento de voz puede funcionar peor con determinados acentos, mientras una herramienta de moderación puede sancionar expresiones culturales fuera de contexto. La ausencia de intención discriminatoria no elimina el impacto. Las plataformas deben

evaluar diferencias en tasas de error, consultar a grupos afectados y corregir patrones que generen desventajas sistemáticas. La igualdad exige comprobar resultados reales y no limitarse a declarar neutralidad tecnológica.

La supervisión humana debe ser real y no meramente formal. Una persona que confirma automáticamente la recomendación del sistema sin revisar contexto no proporciona una garantía efectiva. El revisor debe comprender la función del algoritmo, acceder a información suficiente y poseer autoridad para modificar el resultado. Las decisiones graves, como cancelar una cuenta o bloquear activos, requieren un nivel superior de intervención. La revisión debe realizarse dentro de plazos razonables para evitar que una medida provisional produzca daños permanentes antes de ser corregida.

Zhu et al. (2025) señalan que la supervisión de cajas negras requiere auditoría, acceso a información y capacidad institucional. La auditoría algorítmica permite examinar datos, funcionamiento, resultados y cumplimiento normativo. Puede identificar tasas de error, sesgos, vulnerabilidades y discrepancias entre objetivos declarados y efectos reales. Cheong (2024) destaca que la transparencia necesita mecanismos de control capaces de proteger el bienestar, mientras Papagiannidis et al. (2025) sitúan la auditoría dentro de prácticas de gobernanza aplicables durante todo el ciclo de vida. Los sistemas de mayor impacto deberían someterse a evaluaciones externas con resultados verificables y planes de corrección.

Papagiannidis et al. (2025) integran la trazabilidad y la asignación de funciones dentro de la gobernanza responsable del ciclo de vida. La trazabilidad permite reconstruir cómo se produjo una decisión. Deben conservarse la versión del sistema, los datos relevantes, las reglas aplicadas y las intervenciones humanas realizadas. Esta información facilita revisar errores y determinar responsabilidades. Sin embargo, la trazabilidad no debe justificar el almacenamiento ilimitado de toda la actividad del usuario. Los registros deben limitarse a lo necesario para explicar y auditar decisiones significativas. La conservación debe contar con seguridad, plazos definidos y restricciones de acceso que protejan datos personales y secretos empresariales legítimos.

La robustez y la seguridad forman parte de la responsabilidad algorítmica porque un sistema puede ser manipulado mediante datos falsos, ataques adversariales o accesos privilegiados. Gupta et al. (2023) proponen controles de confianza cero orientados a

verificar identidades, dispositivos y contextos. Estas medidas deben complementarse con pruebas de funcionamiento, registro de incidentes y capacidad para suspender el sistema cuando produzca resultados inesperados. La seguridad técnica no reemplaza la explicabilidad, la supervisión humana ni la reparación de decisiones erróneas.

La transparencia debe extenderse a la personalización de contenidos y publicidad. Los usuarios necesitan saber cuándo una oferta, recomendación o interacción ha sido seleccionada mediante perfiles conductuales. Esto es especialmente importante cuando el sistema utiliza emociones, movimientos o patrones de permanencia para influir en decisiones. Cheong (2024) sostiene que la transparencia algorítmica debe permitir comprender la intervención del sistema y exigir responsabilidades, sin reducirse a avisos generales que no expliquen el funcionamiento relevante.

Los sistemas de moderación algorítmica requieren controles específicos porque pueden restringir libertad de expresión y participación. El análisis automático de voz, gestos o movimientos puede interpretar erróneamente contexto cultural, discapacidad o interacción consentida. Las reglas deben indicar qué conductas se detectan y qué medidas pueden aplicarse. Una alerta automática puede justificar revisión, pero no siempre una sanción definitiva. La persona afectada debe conocer la evidencia esencial, aportar contexto y solicitar una evaluación humana que no dependa únicamente de la clasificación inicial.

Cheong (2024) sostiene que la transparencia solo resulta efectiva cuando se vincula con responsabilidad, participación y posibilidad de cuestionar resultados. La rendición de cuentas exige que la plataforma publique información agregada sobre el funcionamiento de sus sistemas. Puede incluir número de decisiones automatizadas, categorías afectadas, tasas de apelación, errores reconocidos y medidas correctivas. Estos reportes permiten evaluar patrones sin revelar datos personales. Sin embargo, la publicación no debe convertirse en una estrategia reputacional basada en indicadores seleccionados unilateralmente. La información debe ser verificable, comparable y suficientemente detallada para que autoridades, investigadores y usuarios puedan identificar problemas persistentes o grupos afectados de forma desproporcionada.

La reparación algorítmica debe corregir tanto la decisión inicial como sus efectos posteriores. Si una cuenta fue suspendida injustamente, puede ser necesario restablecer acceso, recuperar ingresos y eliminar clasificaciones negativas. Si un perfil incorrecto

influyó en recomendaciones o restricciones, debe rectificarse en todos los sistemas relacionados. La LOPDP (2021) reconoce derechos de rectificación y oposición que resultan relevantes frente a datos e inferencias inexactas. La corrección no puede limitarse a modificar una pantalla cuando el error continúa activo en bases internas.

Zhu et al. (2025) destacan que la regulación de plataformas algorítmicas requiere capacidad pública para comprender redes, incentivos y opacidad técnica. Las autoridades públicas deben contar con capacidades técnicas para supervisar sistemas utilizados por plataformas de gran impacto. La dependencia exclusiva de información proporcionada por las empresas limita la eficacia del control. Se requieren protocolos de auditoría, acceso a documentación y profesionales capaces de interpretar modelos, datos y resultados. La supervisión debe respetar secretos empresariales, pero estos no pueden utilizarse para impedir toda revisión. Cuando un sistema afecta derechos fundamentales, la protección jurídica exige un nivel suficiente de escrutinio independiente y posibilidad de imponer medidas correctivas.

La regulación futura debería diferenciar obligaciones según el nivel de riesgo algorítmico. Los sistemas utilizados para recomendaciones recreativas no requieren los mismos controles que aquellos que bloquean cuentas, clasifican menores o administran activos. Un enfoque proporcional puede exigir documentación básica para funciones de bajo impacto y auditorías independientes para decisiones significativas. También debe prever prohibiciones cuando una práctica resulte incompatible con la dignidad, la autonomía o la igualdad. La innovación no justifica utilizar sistemas opacos en ámbitos donde los errores producen consecuencias difíciles de reparar.

La transparencia y la responsabilidad algorítmica requieren explicaciones comprensibles, datos de calidad, auditorías, supervisión humana y mecanismos efectivos de reparación. Cheong (2024) relaciona explicabilidad, auditoría, participación y rendición de cuentas con la protección del bienestar y la posibilidad de cuestionar decisiones automatizadas. Papagiannidis et al. (2025) añaden que la gobernanza responsable debe operar durante todo el ciclo de vida mediante prácticas estructurales, relacionales y procedimentales. Estas exigencias complementan las garantías reconocidas por la LOPDP (2021).

5.7 Inclusión y sostenibilidad virtual

La inclusión y la sostenibilidad virtual constituyen condiciones esenciales para que el metaverso se desarrolle como un espacio socialmente legítimo y jurídicamente responsable. La expansión de los entornos inmersivos no debe evaluarse únicamente por su capacidad tecnológica o económica, sino también por la posibilidad real de que personas con distintas condiciones sociales, culturales y funcionales participen en igualdad. Peña y Rubio (2024) señalan que los mundos virtuales pueden ampliar oportunidades de interacción y colaboración, aunque también reproducir desigualdades existentes cuando el acceso depende de recursos, conectividad y competencias digitales.

La inclusión digital comienza con la disponibilidad material de dispositivos, conexión y servicios compatibles. Los visores inmersivos, sensores y equipos de alto rendimiento pueden representar costos inaccesibles para numerosos usuarios. Esta barrera económica puede generar una participación estratificada, donde determinados grupos acceden a experiencias avanzadas y otros permanecen limitados a versiones reducidas. La regulación y las políticas públicas deben promover alternativas de bajo costo, compatibilidad con diferentes dispositivos y acceso mediante infraestructuras comunitarias, evitando que el metaverso profundice las brechas tecnológicas existentes.

La conectividad también condiciona la participación efectiva. Los entornos inmersivos suelen requerir redes estables, baja latencia y capacidad elevada de procesamiento. En territorios rurales o sectores con servicios deficientes, estas exigencias pueden excluir a estudiantes, trabajadores y emprendedores. Peña y Rubio (2024) advierten que el potencial social de los mundos virtuales depende de las condiciones materiales que permiten utilizarlos. La inclusión requiere inversiones en infraestructura, cobertura territorial y calidad del servicio, sin asumir que la disponibilidad formal de internet garantiza una experiencia funcional y equitativa.

Las competencias digitales representan otra dimensión de la inclusión. Una plataforma puede ser técnicamente accesible y, sin embargo, resultar incomprensible para personas con poca experiencia tecnológica. La navegación tridimensional, la gestión de identidades y las transacciones digitales exigen conocimientos específicos. Peña y Rubio (2024) destacan la importancia de acompañar las tecnologías inmersivas con procesos educativos y metodologías adaptadas. La alfabetización debe incluir seguridad, privacidad, verificación de información y comprensión de las consecuencias jurídicas derivadas de las acciones realizadas dentro del entorno.

La accesibilidad para personas con discapacidad debe incorporarse desde la etapa de diseño. Las interfaces pueden generar barreras cuando dependen exclusivamente de visión, audición, movimientos precisos o respuestas rápidas. Berrezueta et al. (2025) destacan el valor de avatares, retroalimentación visual, reconocimiento gestual, personalización y entornos adaptativos para personas sordas o con dificultades auditivas, aunque identifican costos, limitaciones técnicas y falta de diseño inclusivo. La accesibilidad debe probarse con usuarios diversos y mantenerse durante las actualizaciones.

La representación mediante avatares puede favorecer la participación al permitir que cada persona elija cómo presentarse. Sin embargo, también puede generar exclusión si las opciones corporales, culturales o funcionales son limitadas. Un sistema que solo ofrece determinados tonos de piel, cuerpos o expresiones reproduce una visión restringida de la diversidad. Castillo et al. (2024) muestran que la identidad digital se construye mediante múltiples atributos. La inclusión requiere personalización suficiente, protección frente a imitaciones y ausencia de penalizaciones por elegir representaciones diferentes de los modelos dominantes.

La diversidad lingüística también condiciona el acceso. Las plataformas globales suelen priorizar determinados idiomas y ofrecer traducciones incompletas para otros. Esto puede afectar comprensión contractual, participación comunitaria y acceso a mecanismos de reclamación. La información jurídica, las normas de conducta y las advertencias de seguridad deben estar disponibles en lenguaje comprensible para los usuarios a quienes se dirige el servicio. Peña y Rubio (2024) destacan que la adaptación lingüística favorece experiencias educativas más significativas y reduce exclusiones vinculadas con comprensión y participación.

Tabla 17
Dimensiones de inclusión y sostenibilidad en los entornos virtuales

Dimensión	Barrera principal	Medida de inclusión	Indicador de evaluación
Acceso económico	Alto costo de dispositivos	Versiones compatibles y programas de acceso	Diversidad socioeconómica de usuarios
Conectividad	Baja velocidad o cobertura limitada	Optimización y alternativas de baja demanda	Participación territorial

Dimensión	Barrera principal	Medida de inclusión	Indicador de evaluación
Competencias digitales	Dificultad de uso y comprensión	Formación y asistencia accesible	Autonomía del usuario
Discapacidad	Interfaces visuales, auditivas o motoras excluyentes	Diseño universal y tecnologías de asistencia	Nivel de accesibilidad
Diversidad cultural	Representaciones limitadas	Avatares y contenidos diversos	Variedad de opciones
Lenguaje	Información disponible en pocos idiomas	Traducción y lenguaje claro	Comprensión efectiva
Participación	Decisiones centralizadas	Consultas y representación comunitaria	Influencia real de usuarios
Consumo energético	Infraestructura intensiva	Eficiencia y energías limpias	Huella ambiental
Renovación tecnológica	Obsolescencia rápida	Reparación y compatibilidad prolongada	Vida útil de dispositivos
Bienestar digital	Uso excesivo y fatiga	Pausas, límites y diseño saludable	Calidad de la experiencia

Nota. La sostenibilidad virtual comprende dimensiones sociales, económicas, tecnológicas y ambientales que deben evaluarse de forma conjunta.

La inclusión exige también considerar la participación de grupos históricamente marginados en las decisiones de diseño y gobernanza. No basta con permitirles ingresar a la plataforma si no pueden influir en reglas, funciones y políticas que afectan su experiencia. Los procesos participativos deben incorporar organizaciones de personas con discapacidad, comunidades rurales, grupos culturales y usuarios con diferentes niveles de alfabetización. Berrezueta et al. (2025) destacan que las comunidades virtuales pueden favorecer cooperación, siempre que la participación no quede concentrada en quienes poseen mayores recursos o conocimiento técnico.

La sostenibilidad social se relaciona con la capacidad del entorno para mantener comunidades seguras, diversas y estables. Un modelo basado exclusivamente en consumo, competencia y atención permanente puede generar exclusión, fatiga y relaciones superficiales. Las plataformas deben promover convivencia, colaboración y mecanismos de apoyo. Peña y Rubio (2024) muestran que los entornos inmersivos pueden fortalecer procesos educativos cuando priorizan interacción significativa. La sostenibilidad no depende únicamente de mantener servidores activos, sino de crear

condiciones donde las personas puedan participar sin agotamiento, abuso o dependencia.

El bienestar digital debe incorporarse como parte de la sostenibilidad. El uso prolongado de dispositivos inmersivos puede producir fatiga visual, desorientación, aislamiento o dificultades para equilibrar actividades virtuales y presenciales. Las plataformas pueden incluir recordatorios, pausas, límites configurables y opciones para reducir estímulos. Estas medidas no deben diseñarse como obstáculos, sino como herramientas de autonomía. Un entorno sostenible evita depender de mecanismos que prolonguen artificialmente la permanencia del usuario y reconoce que la calidad de la experiencia resulta más importante que el tiempo total de conexión.

La sostenibilidad ambiental representa otro desafío. Los centros de datos, dispositivos, redes y operaciones distribuidas consumen energía y recursos materiales. Jauhiainen et al. (2023) vinculan el desarrollo de ciudades y entornos virtuales con debates sobre sostenibilidad y planificación. Las empresas deben evaluar consumo energético, emisiones, fabricación y eliminación de equipos. La transición hacia energías más limpias, la optimización de procesos y la reducción de operaciones innecesarias pueden disminuir el impacto ambiental sin impedir la innovación tecnológica.

La fabricación de visores, sensores y controladores también genera impactos derivados de la extracción de minerales, transporte y residuos electrónicos. La renovación rápida de dispositivos puede volver obsoletos equipos todavía funcionales y aumentar la generación de desechos. Una política sostenible debe promover reparabilidad, actualización de software y compatibilidad prolongada. Los fabricantes deberían informar la vida útil estimada, disponibilidad de repuestos y condiciones de reciclaje. La innovación no debe construirse sobre ciclos de reemplazo acelerado que trasladan costos ambientales y económicos a los usuarios.

La eficiencia tecnológica puede contribuir a reducir estos impactos. El procesamiento local, la compresión de datos, la gestión inteligente de servidores y la adaptación de calidad según el dispositivo disminuyen consumo y necesidades de infraestructura. Sin embargo, la eficiencia no debe utilizarse como argumento para ampliar ilimitadamente el volumen de operaciones. El ahorro obtenido puede perderse si aumenta de forma desproporcionada el número de experiencias, transacciones o dispositivos. La

sostenibilidad requiere evaluar el impacto total y no únicamente mejoras aisladas en rendimiento energético.

La sostenibilidad económica implica que las plataformas puedan mantener servicios sin depender de prácticas abusivas o modelos especulativos. Un entorno financiado exclusivamente mediante publicidad invasiva, venta constante de activos o recopilación intensiva de datos puede resultar insostenible para los usuarios. Madanchian y Taherdoost (2024) relaciona la continuidad de los modelos económicos virtuales con la confianza, la utilidad y la estabilidad del ecosistema. La sostenibilidad exige equilibrio entre rentabilidad, precios accesibles, protección del consumidor y continuidad razonable de los servicios contratados.

Las políticas públicas pueden fomentar inclusión mediante programas de conectividad, formación, investigación y acceso institucional a tecnologías inmersivas. Las universidades, centros comunitarios y bibliotecas pueden ofrecer espacios compartidos que reduzcan barreras económicas. Sin embargo, la inversión debe responder a necesidades reales y no a la simple adopción de tendencias tecnológicas. Peña y Rubio (2024) muestran que el valor educativo depende de la integración pedagógica. De igual manera, la inclusión social requiere objetivos, evaluación y acompañamiento, no solamente adquisición de dispositivos.

La evaluación periódica resulta indispensable para determinar si las medidas de inclusión y sostenibilidad producen resultados efectivos. Las plataformas deberían recopilar indicadores sobre accesibilidad, diversidad de usuarios, consumo energético, abandono y barreras reportadas. Esta información debe utilizarse para corregir diseños y no únicamente para promocionar compromisos corporativos. La evaluación debe combinar datos cuantitativos con consultas a comunidades afectadas. Un entorno puede cumplir estándares técnicos y continuar siendo excluyente si sus reglas, costos o dinámicas sociales impiden una participación significativa.

La regulación futura debe exigir obligaciones proporcionales según tamaño, riesgo e impacto ambiental de las plataformas. Los operadores de gran escala deberían publicar informes sobre accesibilidad, consumo energético, vida útil de dispositivos y medidas de inclusión. También podrían someterse a auditorías independientes y planes de mejora. Las obligaciones no deben impedir la entrada de proyectos pequeños, pero sí evitar que la innovación se base en exclusión o deterioro ambiental. Los incentivos

públicos pueden favorecer tecnologías abiertas, eficientes y compatibles con diferentes capacidades económicas y funcionales.

La inclusión y la sostenibilidad virtual requieren abordar acceso, conectividad, discapacidad, diversidad, bienestar y responsabilidad ambiental. Jauhiainen et al. (2023) ofrecen fundamentos para evaluar sostenibilidad, infraestructura y desarrollo comunitario, mientras Peña y Rubio (2024) permiten examinar inclusión en experiencias educativas inmersivas. Berrezueta et al. (2025) aporta evidencia específica sobre accesibilidad, avatares, reconocimiento gestual y adaptación para personas sordas. La expansión del metaverso será legítima cuando sus beneficios puedan distribuirse de manera amplia, segura y sostenible.

5.8 Regulación futura del metaverso en Ecuador

La regulación futura del metaverso en Ecuador debe construirse como una política jurídica gradual, coordinada y basada en riesgos. No resulta conveniente crear de inmediato una ley excesivamente detallada para una tecnología todavía cambiante. El país ya dispone de normas sobre contratación electrónica, protección de datos, consumo, responsabilidad civil, propiedad intelectual y delitos informáticos que pueden aplicarse a numerosas actividades virtuales. El desafío principal consiste en identificar vacíos, armonizar competencias institucionales y establecer obligaciones específicas para plataformas que desarrollen actividades dirigidas de manera efectiva al mercado ecuatoriano.

La primera prioridad consiste en definir conceptos funcionales y evitar categorías demasiado rígidas. La legislación podría identificar plataforma inmersiva, activo virtual, avatar, operador, proveedor de identidad y servicio dirigido al mercado nacional. Estas definiciones deberían atender a las funciones reales y no a denominaciones comerciales. Ghazinoory et al. (2025) advierten que los mundos virtuales combinan componentes técnicos y jurídicos diferentes. Una definición amplia pero flexible permitiría aplicar obligaciones a nuevos modelos sin reformar constantemente la ley cada vez que cambie una tecnología o una marca.

La segunda prioridad debe ser la coordinación entre instituciones existentes. La Superintendencia de Protección de Datos Personales, las autoridades de consumo, los organismos tributarios, la Fiscalía y las entidades de telecomunicaciones podrían intervenir según la materia. Crear una autoridad completamente nueva podría generar

duplicación y mayores costos institucionales. Resulta más eficiente establecer protocolos de cooperación, intercambio de información y delimitación de competencias. Cada organismo debe actuar dentro de su ámbito, pero contar con mecanismos para remitir casos y desarrollar respuestas conjuntas cuando una conducta afecte simultáneamente varios derechos.

La regulación debería adoptar un enfoque basado en riesgos para diferenciar obligaciones según el impacto de cada plataforma. Un entorno utilizado por menores, que procesa biometría o permite transacciones de alto valor, requiere controles más estrictos que una experiencia recreativa limitada. Las obligaciones pueden variar en materia de auditoría, seguridad, transparencia y supervisión. Zhu et al. (2025) sostienen que la regulación debe adaptarse a las funciones y capacidades reales de los actores. La proporcionalidad evita imponer cargas idénticas a proyectos pequeños y grandes operadores globales.

La transparencia institucional debe ocupar un lugar central. Las plataformas de mayor impacto deberían publicar información sobre reglas de moderación, tratamiento de datos, incidentes de seguridad, decisiones automatizadas y mecanismos de reclamación. Los reportes deben ser comprensibles, verificables y comparables. No basta con publicar documentos extensos o indicadores seleccionados unilateralmente. La autoridad competente debería definir estándares mínimos y exigir correcciones cuando existan omisiones significativas. La transparencia debe funcionar como instrumento de supervisión y no únicamente como estrategia reputacional de las empresas.

El segundo eje corresponde a la validez del consentimiento dentro de interfaces inmersivas. Los usuarios necesitan canales claros para denunciar pérdida de cuentas, errores de moderación, cobros indebidos o afectaciones de identidad. Las plataformas que operen de forma relevante en Ecuador deberían ofrecer atención en español, plazos razonables y procedimientos accesibles. Cuando una decisión afecte activos, reputación o participación profesional, debe existir revisión humana. La reclamación interna no sustituye la posibilidad de acudir ante autoridades administrativas o judiciales, pero puede resolver conflictos de manera temprana y reducir daños continuados.

La primera fase de implementación puede concentrarse en lineamientos obligatorios para actividades de alto riesgo, como tratamiento biométrico, participación de menores y decisiones automatizadas significativas. La LOPDP (2021) y su Reglamento General

(2023) permiten articular evaluaciones de impacto, documentación y medidas de mitigación antes del despliegue. Los sistemas que restrinjan cuentas, clasifiquen usuarios o administren activos deberían ofrecer explicación, revisión humana y registro de las correcciones realizadas.

En una segunda fase correspondería establecer estándares técnicos y contractuales para plataformas dirigidas a menores, mercados virtuales y servicios que custodien activos. Las obligaciones deben incluir configuraciones seguras por defecto, verificación de edad proporcional, límites de contacto, información de precios y procedimientos de recuperación. La supervisión puede graduarse según el tamaño del operador, la intensidad de la recopilación y el valor económico administrado, evitando imponer cargas idénticas a proyectos comunitarios y plataformas globales.

La formación de jueces, fiscales, defensores, reguladores y peritos constituye una condición indispensable. Una norma avanzada tendrá poca eficacia si las instituciones no comprenden registros distribuidos, avatares, biometría o evidencia inmersiva. La capacitación debe combinar derecho, tecnología y protección de derechos humanos. También se requieren guías prácticas sobre preservación de evidencia, valoración de daños y análisis de plataformas. El conocimiento técnico no debe quedar concentrado en empresas privadas, porque ello debilitaría la capacidad estatal para supervisar, investigar y resolver controversias de manera independiente.

La evaluación regulatoria debe realizarse periódicamente. Las autoridades deberían analizar incidentes, reclamaciones, decisiones judiciales y evolución tecnológica antes de reformar obligaciones. Los indicadores pueden incluir tiempo de respuesta, acceso a reparación, incidentes de seguridad, accesibilidad y cumplimiento de transparencia. Una regulación adaptativa no significa inestabilidad permanente, sino revisión basada en evidencia. Los principios constitucionales y las garantías mínimas deben mantenerse, mientras los estándares técnicos pueden actualizarse mediante procedimientos públicos, participación social y justificación suficiente.

La regulación futura del metaverso en Ecuador debe ser gradual, basada en riesgos y apoyada en instituciones existentes. Su finalidad no consiste en repetir todas las reglas sobre datos, contratos, delitos o activos, sino en coordinar su aplicación y cubrir vacíos específicos. El modelo más adecuado combina derechos constitucionales, supervisión pública, autorregulación responsable, cooperación internacional e innovación

controlada. Ecuador puede desarrollar un marco propio si prioriza definiciones funcionales, transparencia, capacidad institucional y mecanismos efectivos de reparación frente a riesgos tecnológicos reales.

REFERENCIAS

Al-Busaidi, A. S., Raman, R., Hughes, L., Albashrawi, M. A., Malik, T., Dwivedi, Y. K., . . . Walton, P. (2024). Redefining boundaries in innovation and knowledge domains: Investigating the impact of generative artificial intelligence on copyright and intellectual property rights. *Journal of Innovation & Knowledge, 9*(4), 100630. https://doi.org/10.1016/j.jik.2024.100630

Alqahtany, S. S., y Syed, T. A. (2024). ForensicTransMonitor: A comprehensive blockchain approach to reinvent digital forensics and evidence management. *Information , 15*(2), 109. https://doi.org/10.3390/info15020109

Asamblea Constituyente del Ecuador. (20 de octubre de 2008). *Constitución de la República del Ecuador.* Asamblea Nacional del Ecuador: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Asamblea Nacional del Ecuador. (22 de octubre de 2009). *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.* Corte Constitucional del Ecuador: https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Ley-Organica-de-Garantias-Jurisdiccionales-y-Control-Constitucional_act_marzo_2020.pdf

Asamblea Nacional del Ecuador. (10 de febrero de 2014). *Código Orgánico Integral Penal.* Asamblea Nacional del Ecuador: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Asamblea Nacional del Ecuador. (22 de mayo de 2015). *Código Orgánico General de Procesos.* Consejo de la Judicatura: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/09/Codigo-Org%C3%A1nico-General-de-Procesos.pdf

Asamblea Nacional del Ecuador. (26 de mayo de 2021). *Ley Orgánica de Protección de Datos Personales.* Ministerio de Telecomunicaciones y de la Sociedad de la Información: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Berrezueta, G. S., Daya, R., y Wagner, S. (2025). Virtual reality in sign language education: Opportunities, challenges, and the road ahead. *Frontiers in Virtual Reality, 6*, 1625910. https://doi.org/10.3389/frvir.2025.1625910

Brenncke, M. (2024). Regulating dark patterns. *Notre Dame Journal of International & Comparative Law, 14*(1), 39-79. https://scholarship.law.nd.edu/ndjicl/vol14/iss1/5/

Castillo, A. J., Tasic, I., y Cano, M. D. (2024). Enhancing digital identity: Evaluating avatar creation tools and privacy challenges for the metaverse. *Information, 15*(10), 624. https://doi.org/10.3390/info15100624

Chawki, M., Basu, S., y Choi, K.-S. (2024). Redefiniendo los límites en el metaverso: Navegando los desafíos del daño virtual y la seguridad del usuario. *Laws, 13*(3), 33. https://doi.org/10.3390/laws13030033

Cheong, B. (2024). Transparency and accountability in AI systems: Safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics, 6*, 1421273. https://doi.org/10.3389/fhumd.2024.1421273

Chow, Y.-W., Susilo, W., Li, Y., Li, N., y Nguyen, C. (2023). Visualization and cybersecurity in the metaverse: A survey. *Journal of Imaging, 9*(1), 11. https://doi.org/10.3390/jimaging9010011

Conferencia de La Haya de Derecho Internacional Privado. (diciembre de 2024). *Private international law aspects of the digital economy: Report*. Documento Preliminar núm. 5: https://assets.hcch.net/docs/0d75731a-66a2-496b-b740-bc5503d6be01.pdf?

Congreso Nacional del Ecuador. (10 de julio de 2000). *Ley Orgánica de Defensa del Consumidor*. Defensoría del Pueblo del Ecuador: https://www.dpe.gob.ec/wp-content/dpetransparencia2012/literala/BaseLegalQueRigeLaInstitucion/LeyOrganicadelConsumidor.pdf

Congreso Nacional del Ecuador. (17 de abril de 2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.* Ministerio de Telecomunicaciones y de la Sociedad de la Información: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Congreso Nacional del Ecuador. (3 de enero de 2003). *Código de la Niñez y Adolescencia*. Consejo de la Judicatura: https://www.igualdad.gob.ec/wp-content/uploads/downloads/2017/11/codigo_ninezyadolescencia.pdf

Congreso Nacional del Ecuador. (24 de junio de 2005). *Código Civil*. Defensoría Pública del Ecuador: https://webhistorico.epn.edu.ec/wp-content/uploads/2015/06/Codigo-Civil1.pdf

Fernandez, C., y Hui, P. (2022). Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse. *AI and Ethics*, *2*, 395–404. https://doi.org/10.1109/ICDCSW56584.2022.00058

Fiaz, F., Sajjad, S., Iqbal, Z., Yousaf, M., y Muhammad, Z. (2024). MetaSSI: A framework for personal data protection, enhanced cybersecurity and privacy in metaverse virtual reality platforms. *Future Internet, 16*(5), 159. https://doi.org/10.3390/fi16050176

Ghazinoory, S., Parvin, F., Saghafi, F., Afshari-Mofrad, M., Ghazavi, N., y Fatemi, M. (2025). Metaverse technology tree: A holistic view. *Frontiers in Artificial Intelligence, 8*, 1545144. https://doi.org/10.3389/frai.2025.1545144

González, T. M. (2023). Virtual emotions and criminal law. *Frontiers in Psychology, 14*, 1260425. https://doi.org/10.3389/fpsyg.2023.1260425

Gupta, A., Khan, H., Nazir, S., Shafiq, M., y Shabaz, M. (2023). Metaverse security: Issues, challenges and a viable ZTA model. *Electronics, 12*(2), 391. https://doi.org/10.3390/electronics12020391

Jauhiainen, J., Krohn, C., y Junnila, J. (2023). Metaverse and sustainability: Systematic review of scientific publications until 2022 and beyond. *Sustainability, 15*(1), 346. https://doi.org/10.3390/su15010346

Kasiyanto, S., y Kilinc, M. (2022). The legal conundrums of the metaverse. *Journal of Central Banking Law and Institutions, 1*(2), 299–322. https://doi.org/10.21098/jcli.v1i2.25

Kostenko, O., Furashev, V., Zhuravlov, D., y Dniprov, O. (2022). Genesis of legal regulation web and the model of the electronic jurisdiction of the metaverse. *Bratislava Law Review*, *6*(2), 21–36. https://doi.org/10.46282/blr.2022.6.2.316

Küsters, A. (2026). Trusted but not trustworthy: A conceptual analysis of AI agent risks in the metaverse and EU policy responses. *Frontiers in Virtual Reality, 7*, 1813331. https://doi.org/10.3389/frvir.2026.1813331

Lazea, G., Balea-Stanciu, M., Bunget, O., Sumănaru, A., y Coraș, A. (2025). Cryptocurrency taxation: A bibliometric analysis and emerging trends. *International Journal of Financial Studies, 13*(1), 37. https://doi.org/10.3390/ijfs13010037

Madanchian, M., y Taherdoost, H. (2024). Business model evolution in the age of NFTs and the metaverse. *Information, 15*(7), 378. https://doi.org/10.3390/info15070378

Martínez, L. W., Moreno, B. A., y Ruiz, D. E. (2024). Linking a digital asset to an NFT—Technical and legal analysis. *Laws, 13*(5), 59. https://doi.org/10.3390/laws13050059

Munn, N., y Weijers, D. (2023). The real ethical problem with metaverses. *Frontiers in Human Dynamics, 5*, 1226848. https://doi.org/10.3389/fhumd.2023.1226848

Ness, S. (2024). VAT/GST harmonisation challenges for digital assets such as bitcoin and NFTs in the EU following Case C-264/14 (Skatteverket v David Hedqvist). *International Cybersecurity Law Review, 5*(3), 459–490. https://doi.org/10.1365/s43439-024-00124-2

Papagiannidis, E., Mikalef, P., y Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems, 34*(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885

Peña, A. B., y Rubio, A. F. (2024). Ethical approach to the use of immersive technologies: Advance about digitalisation of multilingual programs in the EHEA. *Frontiers in Virtual Reality, 5*, 1357595. https://doi.org/10.3389/frvir.2024.1357595

Pooyandeh, M., Han, K. J., Sohn, I., y Stylios, C. (2022). Cybersecurity in the AI-based metaverse: A survey. *Applied Sciences, 12*(24), 12993. https://doi.org/10.3390/app122412993

Sakka, S., Liagkou, V., y Ferreira, A. (2026). Digital boundaries and consent in the metaverse: A comparative review of privacy risks. *Journal of Cybersecurity and Privacy*, *6*(1), 24. https://doi.org/10.3390/jcp6010024

Santamaría, P., Tobarra, L., Pastor-Vargas, R., y Robles-Gómez, A. (2023). Smart contracts for managing the chain-of-custody of digital evidence: A practical case of study. *Smart Cities*, *6*(2), 709–727. https://doi.org/10.3390/smartcities6020034

Sentencia 001-14-PJO-CC, 0067-11-JD (Corte Constitucional del Ecuador 23 de abril de 2014). http://bivicce.corteconstitucional.gob.ec/local/File/Gaceta_Constitucional/007_Gaceta_Constitucional_no_007_03-07-2014.pdf

Sentencia 182-15-SEP-CC, 1493-10-EP (Corte Constitucional del Ecuador 28 de septiembre de 2015). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoicm8iLCJ1dWlkIjoiODhmMGY4ZmQtN2YzNS00Y2FhLTkxOWEtNjhhZjE2MDRmZjA2LnBkZiJ9

Sentencia 2064-14-EP/21, 2064-14-EP (Corte Constitucional del Ecuador 27 de enero de 2021). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoidHJhbWl0ZSIsInV1aWQiOiI1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmIn0=

Sentencia 47-19-JD/22, 47-19-JD (Corte Constitucional del Ecuador 21 de diciembre de 2022). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic4ZTM4ZGFhOC1hY2NiLTQ0NjktOTcyNy1jZTZjOWIyNzUxNTYucGRmJ30=

Sentencia 59-19-IN/24, 59-19-IN (Corte Constitucional del Ecuador 11 de julio de 2024). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoidHJhbWl0ZSIsInV1aWQiOiJjODcwOTNhZS04ZTExLTRjNGQtOTMxOC01ZTc3NDJlOGFiMTYucGRmIn0=

Sentencia 89-19-JD/21, 89-19-JD (Corte Constitucional del Ecuador 20 de julio de 2021). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic2MWI1ZDhiMy1iYmE1LTRhN2UtOWZjNS02NzM1ZWFiMzVlNTYucGRmJ30=

Smith, C., Molka-Danielsen, J., Webb-Benjamin, J., y Rasool, J. (2025). The challenges of consent in a decentralised metaverse: Exploring ethically informed protections and standards to safeguard humans. *Frontiers in Blockchain, 8*, 1471431. https://doi.org/10.3389/frvir.2025.1401073

Song, C., Shin, S., y Shin, K. (2023). Exploring the key characteristics and theoretical framework for research on the metaverse. *Applied Sciences, 13*(13), 7628. https://doi.org/10.3390/app13137628

Sorrentino, G., y López, G. J. (2025). Rethinking privacy for avatars: Biometric and inferred data in the metaverse. *Frontiers in Virtual Reality, 6*, 1520655. https://doi.org/10.3389/frvir.2025.1520655

Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. *Information, 14*(2), 117. https://doi.org/10.3390/info14020117

Tukur, M., Schneider, J., Househ, M., Dokoro, A., Ismail, U., Dawaki, M., y Agus, M. (2023). The metaverse digital environments: A scoping review of the challenges, privacy and security issues. *Frontiers in Big Data, 6*, 1301812. https://doi.org/10.3389/fdata.2023.1301812

Varela, E. C., Toasa, R., y Urdaneta, M. (2025). The use of artificial intelligence in cybercrime: Impact analysis in Ecuador and mitigation strategies. *Journal of Cybersecurity and Privacy, 5*(4), 100. https://doi.org/10.3390/jcp5040100

Wang, X., Lee, L. H., Bermejo, F. C., y Hui, P. (2024). The Dark Side of Augmented Reality: Exploring Manipulative Designs in AR. *International Journal of Human–Computer Interaction, 40*(13), 3449-3464. https://doi.org/10.1080/10447318.2023.2188799

Zhu, G., Tang, M., Jian, X., y Mu, T. (2025). A study of government regulation's strategy for solving the algorithmic black-box puzzle of digital platforms: A

complex network-based perspective. *Frontiers in Physics*, *13*, 1538742. https://doi.org/10.3389/fphy.2025.1538742

Derecho y metaverso

frente a los desafíos de los mundos virtuales

Esta obra analiza los principales desafíos que el metaverso plantea al derecho, con especial atención al ordenamiento jurídico ecuatoriano. Se examinan la identidad digital, los avatares, la protección de datos personales y biométricos, el consentimiento, la intimidad, la libertad de expresión, la protección de menores, la suplantación de identidad y el hábeas data. Asimismo, se estudian la economía virtual, los bienes digitales, la propiedad de activos, los NFT, los contratos electrónicos e inteligentes, la protección del consumidor, la propiedad intelectual y la tributación de operaciones virtuales.





ISBN: 978-9907-848-12-0

9 789907 848120

CIDPROS
EDITORIAL