

El derecho a la autenticidad de la información

Una institución pendiente para la economía digital

“Así como los derechos de propiedad seguros se convirtieron en uno de los fundamentos institucionales de las economías modernas, la comunicación digital confiable se está convirtiendo en uno de los fundamentos institucionales de la economía digital y de la era de la inteligencia artificial.”

Luis Ángel Rodríguez Alemán

Ingeniero en Computación · Maestro en Políticas Públicas · Maestro en Planeación Regional y Urbana
Fundador de AliPsé

Agosto de 2026

Nota de publicación

Este documento propone el derecho a la autenticidad de la información como un principio normativo e institucional para la economía digital. No sostiene que dicho derecho se encuentre ya reconocido de manera universal en el derecho positivo, ni pretende sustituir los derechos de autor, la protección de datos personales, la libertad de expresión, el debido proceso o las reglas existentes sobre evidencia y firmas electrónicas. Su propósito es abrir una conversación interdisciplinaria entre juristas, tecnólogos, economistas, filósofos, responsables de políticas públicas, organismos de desarrollo, empresas, creadores y ciudadanos.

El ensayo distingue cuidadosamente entre autenticidad y verdad. Una comunicación puede ser auténtica y, sin embargo, equivocada; también puede ser verdadera y no encontrarse registrada. La capacidad propuesta es más acotada: que una persona o institución legítima pueda demostrar qué contenido emitió realmente, y que quienes reciben ese contenido dispongan de una oportunidad práctica para verificarlo sin renunciar a su libertad para interpretarlo, criticarlo, transformarlo o rechazarlo.

Título	El derecho a la autenticidad de la información: una institución pendiente para la economía digital
Serie	AliPsé White Paper No. 1
Autor	Luis Ángel Rodríguez Alemán
Versión	Edición para publicación, agosto de 2026
Cita sugerida	Rodríguez Alemán, Luis Ángel (2026). El derecho a la autenticidad de la información: una institución pendiente para la economía digital. AliPsé White Paper No. 1.

© 2026 Luis Ángel Rodríguez Alemán / AliPsé. Se autoriza la cita y reproducción parcial con atribución adecuada. La reproducción íntegra, traducción o adaptación para fines comerciales requiere autorización previa. Contacto: luisangel@alipse.net · www.alipse.net

Resumen

Internet se convirtió en la infraestructura dominante para distribuir información sin adquirir una infraestructura igualmente universal para autenticarla. Esa brecha arquitectónica permitió desde el inicio la falsificación, la suplantación y la manipulación; la inteligencia artificial generativa no creó el problema, pero sí lo industrializó al reducir de forma radical su costo, tiempo y dificultad técnica.

Este ensayo sostiene que la autenticidad de la información no es únicamente un problema tecnológico. Es una condición de posibilidad para la cooperación humana a gran escala. La principal fortaleza del Homo sapiens no radica en su capacidad física individual, sino en su aptitud para coordinarse con grandes números de personas, compartir conocimiento, crear instituciones y actuar sobre realidades comunes. Esa cooperación depende del lenguaje, de la atribución de responsabilidades y de un grado suficiente de confianza en la identidad de las fuentes, la integridad de los mensajes y la continuidad de su procedencia.

Se propone, por ello, el derecho a la autenticidad de la información: un principio normativo e institucional conforme al cual toda persona u organización debería disponer de medios razonables para establecer, preservar y demostrar cuáles fueron los contenidos, palabras, imágenes, sonidos o comunicaciones que efectivamente emitió, así como para distinguirlos de versiones alteradas, fabricadas o falsamente atribuidas. El derecho propuesto protege la atribución y la integridad de la comunicación; no concede infalibilidad al emisor ni autoriza la imposición de una verdad oficial.

El documento examina la dimensión digital como extensión instrumental de la vida física —la “dimensión 4.5” planteada por el autor—; analiza los costos personales, económicos, democráticos e institucionales de la inautenticidad; propone una arquitectura abierta de registros, certificación, verificación pública y detección; y formula salvaguardas para evitar censura, vigilancia, centralización y falsas certezas. AliPsé aparece al final como una hipótesis concreta de implementación de una institución que, por su importancia, debe trascender a cualquier empresa, gobierno o plataforma individual.

Palabras clave: autenticidad de la información; fake news; confianza digital; cooperación humana; procedencia; integridad de contenidos; dimensión 4.5; infraestructura pública digital; inteligencia artificial generativa; resiliencia institucional; criptografía poscuántica.

Índice

Prólogo. El derecho a nuestras propias palabras	5	11. Gobiernos, servicios públicos y comunicación institucional	12
1. Civilización, cooperación e instituciones	5	12. Democracia, elecciones y esfera pública	12
2. Internet: el megáfono más poderoso de la historia	6	13. La institución pendiente de la economía digital	13
3. Lo líquido, lo efímero y la fragilidad de la palabra	7	14. Principios de una infraestructura de autenticidad	13
4. La dimensión 4.5 de la existencia humana	7	15. Riesgos, salvaguardas y límites	14
5. La evolución histórica de la crisis de autenticidad	8	16. AliPsé como hipótesis de implementación	15
6. Las palabras, las ideas y la identidad comunicativa	9	Conclusión. ¿Quién protegerá nuestras palabras?	16
7. Autenticidad no es verdad	9	Notas y referencias	18
8. El derecho a la autenticidad de la información	10	Bibliografía y fuentes institucionales seleccionadas	19
9. De la certeza sobre la propiedad a la certeza sobre la atribución	10	Sobre el autor	20
10. Los costos sociales y económicos de la inautenticidad	11		

Prólogo

¿Qué significa conservar el derecho a nuestras propias palabras?

El derecho a nuestras propias palabras

La idea que con el tiempo se convertiría en AliPsé comenzó a tomar forma durante el encierro provocado por la pandemia de COVID-19. En aquellos meses, buena parte de la vida humana cambió de escenario casi de un día para otro: el trabajo, la educación, la información sanitaria, el comercio, las relaciones personales, la deliberación pública y hasta los rituales más íntimos de una sociedad se trasladaron a la dimensión digital.

El encierro hizo visible, además, otra transformación menos evidente. En un mundo marcado por la velocidad, la inestabilidad y la sustitución continua, parecía cada vez más difícil conservar un dominio real sobre aquello que considerábamos propio. Los empleos podían desaparecer; los vínculos se volvían más frágiles; las plataformas controlaban datos, audiencias y memoria; las imágenes circulaban fuera de contexto; una frase podía ser recortada hasta adquirir el sentido opuesto; una captura de pantalla podía sobrevivir a su fuente; una cuenta falsa podía hablar con la voz de una persona real.

De esa observación surgió una intuición muy sencilla: aun si la vida contemporánea vuelve más incierta la propiedad de muchas cosas, las personas deberían conservar, por lo menos, el derecho a sus propias palabras. Debería existir una forma confiable de demostrar: “Esto fue lo que realmente dije”, “Esta fue la imagen que publiqué”, “Este comunicado salió de mi institución”, “Estas palabras nunca fueron mías”.

La palabra no es un objeto trivial. A través de ella expresamos ideas, intenciones, compromisos, conocimientos, afectos, desacuerdos y proyectos. Las personas no se reducen a sus palabras, pero una parte sustancial de su identidad pública, de su pensamiento compartido y de su capacidad para participar en la vida social se manifiesta por medio de ellas. Cuando alguien logra colocar palabras falsas en la boca de otro y hacerlas indistinguibles de las auténticas, no altera únicamente un archivo: interviene la continuidad de su identidad comunicativa.

Este ensayo parte, por ello, de una pregunta que parece tecnológica, pero que en realidad es civilizatoria:

En una civilización que ha construido instituciones para proteger la propiedad, los contratos, la identidad y la moneda, ¿qué institución protege la autenticidad de las palabras, ideas y comunicaciones de las personas y organizaciones en la dimensión digital?

La respuesta que se desarrolla en las páginas siguientes es incómoda: esa institución todavía no existe de manera universal, accesible, interoperable e independiente. Y mientras continúe pendiente, el problema no permanecerá estático. Como ocurre con muchas carencias institucionales, tenderá a agravarse con el paso del tiempo, la expansión de la vida digital y el desarrollo de tecnologías capaces de fabricar con precisión creciente la apariencia de lo auténtico.

1. Civilización, cooperación e instituciones

¿Qué permitió a los seres humanos cooperar más allá de los pequeños grupos?

La civilización es, en buena medida, una obra de cooperación acumulada. Ningún individuo, por inteligente o hábil que sea, puede construir por sí solo una ciudad, una universidad, un sistema de salud, una red eléctrica, una ciencia acumulativa o un Estado de derecho. Las sociedades prosperan cuando coordinan esfuerzos entre personas que no se conocen, viven en lugares distintos e incluso pertenecen a generaciones diferentes.

Yuval Noah Harari ha popularizado la tesis de que la ventaja singular del Homo sapiens no consiste simplemente en cooperar —muchas especies lo hacen—, sino en cooperar con flexibilidad y en grandes números mediante relatos, reglas e instituciones compartidas.¹

Esa capacidad de coordinación no depende solo de la inteligencia individual. Depende del lenguaje, de la memoria, de la posibilidad de hacer promesas, atribuir responsabilidades y compartir representaciones de la realidad. Una sociedad puede organizar impuestos, hospitales, escuelas, elecciones o cadenas de suministro porque millones de personas reconocen símbolos, reglas, autoridades, documentos y declaraciones dotados de un significado suficientemente común.

La cooperación es uno de los grandes poderes de nuestra especie. El lenguaje hizo posible esa cooperación; las instituciones la extendieron más allá de los pequeños grupos; y la confianza permitió sostenerla a través del tiempo. De ahí se desprende una proposición central de este ensayo:

La cooperación humana a gran escala depende de la comunicación; la comunicación capaz de coordinar acciones requiere un grado suficiente de confianza; y esa confianza se deteriora cuando ya no podemos distinguir las palabras auténticamente emitidas de las falsamente atribuidas.



Figura 1. Cadena conceptual de la cooperación humana a gran escala.

Las instituciones cumplen precisamente una función de estabilización. Douglass C. North las describió como las reglas formales e informales que estructuran la interacción humana y reducen la incertidumbre. Los derechos de propiedad aclaran titularidades; los contratos hacen exigibles compromisos; los registros públicos preservan actos y estados jurídicos; los tribunales resuelven controversias; las instituciones monetarias sostienen expectativas sobre el valor.²

No todas las instituciones son justas, eficaces o neutrales. Algunas distribuyen poder de manera desigual; otras preservan privilegios o se vuelven obsoletas. Pero la lección general sigue siendo válida: sin mecanismos creíbles para establecer derechos, responsabilidades y registros, aumentan los costos de coordinarse y disminuye la capacidad de planear a largo plazo.

La autenticidad informativa pertenece, por ello, a una conversación sobre instituciones y no solamente sobre software. Cuando una comunicación puede ser atribuida falsamente a un emisor sin que exista un método práctico para confrontarla con una versión autorizada, se incrementa la incertidumbre sobre una de las materias primas de la cooperación: quién dijo qué, cuándo y en qué forma.

2. Internet: el megáfono más poderoso de la historia

¿Qué cambió cuando cualquiera pudo hablar con millones de desconocidos?

Nunca antes en la historia una sola persona había podido hablar, al mismo tiempo, con millones de desconocidos. Durante siglos, alcanzar una audiencia masiva exigió controlar una imprenta, una estación de radio, un canal de televisión, una editorial o una estructura política. Internet redujo de manera radical esas barreras. Una persona con un teléfono puede dirigirse a una comunidad, documentar un abuso, organizar ayuda, crear conocimiento o participar en una conversación global.

Esta capacidad ha tenido consecuencias políticas profundas. Movimientos sociales, protestas, campañas y redes de solidaridad han utilizado la conectividad digital para coordinar acciones y desafiar monopolios tradicionales de información.

El poder de Internet no reside solamente en transportar mensajes, sino en alterar quién puede producirlos, quién puede recibirlos y con qué rapidez pueden generar una respuesta colectiva.

Pero el mismo diseño que favorece la apertura, la copia y la recombinación dificulta conservar la procedencia. Un archivo puede descargarse, recortarse, traducirse, recomprimirse y volver a publicarse. Una declaración puede separarse de su contexto. Una imagen auténtica puede acompañarse de un pie falso. Un audio puede editarse para invertir su sentido. El contenido conserva su fuerza persuasiva aunque pierda su historia.

La red se volvió extraordinariamente eficiente para responder a la pregunta “¿cómo hago llegar este mensaje a millones de personas?”, pero no desarrolló una respuesta igualmente sencilla para “¿cómo demuestro que este fue realmente mi mensaje?”.

La humanidad obtuvo el megáfono más poderoso de su historia sin construir, al mismo tiempo, una capacidad ampliamente disponible para preservar y comprobar la continuidad entre la fuente, el mensaje y las versiones que llegan a sus audiencias. Esa asimetría constituye la raíz arquitectónica de la crisis de autenticidad.

3. Lo líquido, lo efímero y la fragilidad de la palabra

¿Qué ocurre con la autoría cuando todo circula, cambia y se recontextualiza?

La vida contemporánea parece haber perdido buena parte de sus antiguas formas sólidas. Zygmunt Bauman utilizó la metáfora de la “modernidad líquida” para describir el tránsito hacia condiciones marcadas por la flexibilidad, la incertidumbre, la movilidad y la fragilidad de los vínculos. En sus obras, la liquidez alcanza el trabajo, la identidad, las relaciones, el consumo y la experiencia misma del tiempo.³

No es necesario aceptar todas las implicaciones de esa teoría para reconocer que buena parte de la vida contemporánea se experimenta como provisional. Las plataformas cambian sus reglas; las identidades digitales se fragmentan; la memoria se externaliza; los vínculos laborales y afectivos se reorganizan; lo publicado puede desaparecer y, paradójicamente, también puede permanecer para siempre fuera del control de quien lo emitió.

En este entorno, incluso la palabra propia se vuelve líquida. Puede circular sin soporte estable, desprenderse de su contexto y adquirir versiones sucesivas. La fragilidad no reside solo en que las palabras desaparezcan, sino en que continúen existiendo bajo formas que ya no corresponden a lo emitido y cuya atribución puede seguir pareciendo auténtica.

El mundo digital combina, de manera paradójica, lo efímero y lo imborrable. Un mensaje puede ser visible solo por segundos y, al mismo tiempo, ser capturado, reproducido y recontextualizado indefinidamente. Esta tensión vuelve insuficiente la idea tradicional de que el desmentido posterior corrige el daño. La falsificación puede haber alcanzado a millones antes de que el original sea localizado; la versión manipulada puede sobrevivir al contexto que permitía comprenderla.

La modernidad líquida no causa la crisis de autenticidad, pero ayuda a comprender el ambiente cultural en el que esta se desarrolla: un mundo donde la permanencia, la autoría y la continuidad de las cosas resultan más difíciles de asegurar. Precisamente por ello, la sociedad digital necesita instituciones capaces de hacer verificable aquello que ya no puede hacer sólido.

4. La dimensión 4.5 de la existencia humana

¿Por qué importa proteger la autenticidad en la dimensión digital?

La vida digital ya no ocurre fuera de la vida. Trabajamos, aprendemos, compramos, ahorramos, nos relacionamos, ejercemos derechos, construimos reputación y participamos políticamente en espacios digitales. Una parte creciente de las consecuencias que experimentamos en el mundo físico se origina en interacciones que comenzaron en una pantalla.

He llamado “dimensión 4.5” a esta condición. No se trata de una dimensión completamente separada de la vida física, ni de una simple metáfora espacial. Es una extensión instrumental de nuestra existencia: un ámbito que multiplica las posibilidades del mundo material, elimina parcialmente las restricciones de distancia y tiempo, y produce efectos que regresan

continuamente al cuerpo, la economía, la reputación, la salud y la vida política. El concepto fue desarrollado inicialmente en el capítulo “La informática en un mundo interdisciplinario” (Rodríguez Alemán, 2016).

El término 4.5 busca reflejar esa condición intermedia. La dimensión digital no sustituye las dimensiones físicas ni constituye una realidad autosuficiente; pero tampoco puede reducirse a un canal secundario. Una decisión bancaria tomada en línea modifica patrimonio físico. Una falsificación difundida en una red puede provocar violencia en una calle. Una alerta sanitaria digital puede salvar vidas. Un comunicado apócrifo puede mover mercados o alterar una elección.

La importancia de proteger la autenticidad en la dimensión digital se deriva, por tanto, de una razón elemental: esa dimensión ya forma parte de la vida humana. Preguntar por qué importa proteger las palabras en Internet equivale, en buena medida, a preguntar por qué importa proteger las acciones, los derechos y las identidades de las personas en cualquier ámbito donde su existencia produzca consecuencias reales.

Si los derechos y las instituciones fueron creados para hacer más segura la vida física, sus equivalentes funcionales deben extenderse al espacio donde transcurre una parte creciente de esa vida. Identidad, privacidad, propiedad, evidencia, seguridad y autenticidad no pierden relevancia al cruzar una pantalla; al contrario, necesitan ser reconstruidas para un medio cuyas propiedades son diferentes.

5. La evolución histórica de la crisis de autenticidad

¿Cómo pasó la falsificación de ser una práctica costosa a una capacidad industrial?

La falsificación es antigua. Su escala contemporánea no lo es. La historia humana está llena de documentos apócrifos, rumores, propaganda, suplantaciones y relatos atribuidos a autoridades que nunca los emitieron. Lo que ha cambiado no es la existencia del engaño, sino su economía: quién puede producirlo, cuánto cuesta, con qué velocidad circula y qué tan convincente puede llegar a ser.

Puede distinguirse una evolución acumulativa en cuatro etapas. Cada una añade capacidades y riesgos sin sustituir por completo a las anteriores:

Etapas 1 — Comunicación analógica

La manipulación era posible, pero solía exigir acceso a medios físicos, habilidades especializadas o canales de distribución. La falsificación de una fotografía, un documento o una grabación podía ser costosa y dejar huellas materiales. La escala estaba limitada por imprentas, cintas, laboratorios, transmisores o redes organizativas.

Etapas 2 — Digitalización e Internet

Copiar, editar y redistribuir se volvió barato. La copia digital perdió las diferencias visibles respecto del original. El contenido pudo circular globalmente y separarse de su soporte, fecha, autor y contexto. La red hizo posible que una alteración realizada por una sola persona llegara a audiencias antes reservadas a grandes organizaciones.

Etapas 3 — Redes sociales y mensajería instantánea

La distribución se volvió algorítmica, emocional y casi inmediata. El contenido dejó de viajar principalmente como publicación formal y comenzó a hacerlo como fragmento reenviado, captura, meme, clip o audio. La velocidad de propagación superó la capacidad de comprobación, mientras las señales sociales —quién lo envía, cuántas veces se comparte, cuánta indignación produce— comenzaron a sustituir a la evidencia de origen. El fenómeno popularmente descrito como fake news es una manifestación visible de esta transformación, pero no agota el problema institucional que la hizo posible.

Etapas 4 — Inteligencia artificial generativa

La fabricación convincente se volvió accesible, automatizable y escalable. Voces, rostros, estilos de escritura, documentos y escenas pueden sintetizarse o alterarse con una inversión mínima. Un atacante puede producir múltiples variantes adaptadas a idiomas, audiencias y plataformas. La inteligencia artificial no creó la crisis de autenticidad: la industrializó.

Esta evolución muestra por qué las respuestas centradas exclusivamente en “detectar contenido generado por IA” son insuficientes. Las instituciones legítimas también utilizan herramientas generativas para crear materiales oficiales; los actores

maliciosos combinan IA con edición tradicional; y una falsificación puede construirse desde cero o derivarse de un original auténtico. La pregunta operativa no es qué marca de software produjo el archivo. Es si el contenido que circula corresponde a una versión de referencia que la fuente legítima registró o reconoció como propia.



Figura 2. Evolución acumulativa de la crisis de autenticidad.

6. Las palabras, las ideas y la identidad comunicativa

¿Qué protegemos realmente cuando protegemos la autenticidad de las palabras?

Las palabras no solo describen el mundo: también actúan sobre él. Con ellas prometemos, ordenamos, autorizamos, educamos, condenamos, perdonamos, contratamos, legislamos y organizamos. Buena parte de la vida institucional existe porque determinadas palabras son pronunciadas o registradas por personas investidas de una capacidad reconocida.

Una ley es lenguaje. Un contrato es lenguaje. Una sentencia es lenguaje. Un título académico, una receta médica, una alerta de emergencia y un comunicado de un banco central son expresiones simbólicas que producen efectos porque una comunidad reconoce su origen y autoridad.

Wittgenstein escribió que los límites de su lenguaje significaban los límites de su mundo. Hannah Arendt situó la palabra y la acción en el centro de la aparición pública de las personas. Habermas construyó una teoría de la acción comunicativa en la que la cooperación social depende de pretensiones de validez susceptibles de ser discutidas.⁴

No es necesario afirmar que las personas “son” únicamente sus palabras. Somos también cuerpo, memoria, relaciones, acciones y silencios. Pero una parte sustancial de nuestra identidad pública y de nuestra participación social se expresa mediante comunicaciones que otros nos atribuyen. La continuidad de esa atribución forma lo que aquí puede llamarse identidad comunicativa: la posibilidad de ser reconocidos, a través del tiempo, por aquello que realmente dijimos, publicamos, autorizamos o negamos.

Cuando una sociedad pierde la capacidad de distinguir las palabras auténticamente emitidas por una persona de aquellas falsamente atribuidas, no solo se pone en riesgo una reputación. Se deteriora uno de los mecanismos mediante los cuales las personas cooperan, deliberan, asumen responsabilidad y construyen memoria común.

Proteger la autenticidad de nuestras palabras es proteger la infraestructura simbólica de la cooperación humana.

7. Autenticidad no es verdad

¿Puede una comunicación ser auténtica y, sin embargo, equivocada?

Autenticidad y verdad no son lo mismo. Esta es la distinción más importante del ensayo. Una comunicación auténtica es aquella que corresponde realmente a la fuente a la que se atribuye. Eso no garantiza que su contenido sea correcto, completo, legal, moral o científicamente verdadero.

Un gobierno puede emitir auténticamente una estadística equivocada. Una empresa puede publicar de manera auténtica una promesa que después incumple. Una persona puede decir con autenticidad algo falso. La infraestructura de autenticidad no convierte esas afirmaciones en verdad; únicamente permite establecer que fueron efectivamente emitidas por esa fuente.

Esta limitación no debilita el derecho propuesto. Lo vuelve viable y compatible con una sociedad plural. Una infraestructura que intentara determinar la verdad absoluta de todas las afirmaciones tendría que concentrar un poder epistemológico y político incompatible con la libertad. En cambio, una infraestructura que demuestre procedencia resuelve una pregunta más acotada y verificable: “¿Este contenido coincide con la versión emitida por esta fuente?”

Conviene distinguir cuatro conceptos que suelen confundirse. La identidad responde quién reclama ser la fuente; la integridad indica si los bits o la evidencia han cambiado; la procedencia reconstruye el origen y las transformaciones conocidas; y la autenticidad expresa la correspondencia suficientemente sustentada entre un contenido y la fuente a la que se atribuye. Ninguno de estos elementos, por sí solo, determina la verdad de lo afirmado.

La autenticidad tampoco sustituye al periodismo, la ciencia, los tribunales, el debate público o la verificación de hechos. Los complementa. Primero puede establecerse qué dijo realmente una institución; después puede discutirse si tenía razón, si actuó legalmente o si su afirmación merece confianza.

Esta distinción evita que el derecho a la autenticidad se convierta en un “ministerio de la verdad”. La infraestructura no debe decidir qué ideas pueden circular, sino hacer visible la relación entre un contenido y su fuente. La crítica, la sátira, la parodia, la cita, la transformación y el desacuerdo deben permanecer abiertos, siempre que no se presenten engañosamente como el original inalterado.

8. El derecho a la autenticidad de la información

¿Qué facultades mínimas debería reconocer una institución de autenticidad?

La propuesta puede expresarse con sencillez: toda persona y toda organización deberían contar con medios proporcionados para demostrar cuáles fueron realmente sus comunicaciones. A ese principio normativo y a la capacidad institucional que busca hacerlo efectivo los llamamos aquí derecho a la autenticidad de la información:

Toda persona u organización debería disponer de una capacidad práctica para establecer, preservar y demostrar de manera verificable cuáles fueron los contenidos, palabras, imágenes, sonidos o comunicaciones que efectivamente emitió; y toda persona que reciba esos contenidos debería disponer de una oportunidad razonable para comprobar si corresponden a una versión de referencia reconocida por la fuente.

En su etapa inicial, este derecho debe entenderse como una aspiración institucional y un criterio de diseño, no como la afirmación precipitada de una nueva causa de acción universal. Puede orientar estándares, arquitectura tecnológica, contratación pública, gobernanza corporativa, investigación y políticas públicas antes de que exista cualquier reconocimiento jurídico general.

El derecho propuesto contiene al menos cuatro dimensiones:

Estas dimensiones no deben entenderse necesariamente como cuatro derechos subjetivos independientes. Funcionan, en esta etapa, como componentes de una misma capacidad institucional y como criterios para evaluar normas, productos y políticas públicas.

1. Constancia de emisión: la capacidad de dejar evidencia de qué comunicación fue emitida por una fuente legítima o autorizada.
2. Preservación: la capacidad de conservar evidencia durable de la versión emitida, incluso cuando cambien las plataformas, los formatos o los responsables institucionales.
3. Verificación: la posibilidad de que terceros comprueben la correspondencia con una referencia registrada mediante canales accesibles, sin depender exclusivamente de una declaración posterior del propio emisor.
4. Deslinde verificable: la capacidad de aportar evidencia de que una versión fabricada, alterada o falsamente atribuida no corresponde a la comunicación registrada por la fuente.

Una implementación madura debería evitar el falso binarismo y contemplar, al menos, cuatro resultados: coincidencia auténtica; alteración material detectada; contenido no encontrado; y evidencia insuficiente. La ausencia de un registro no prueba falsedad, del mismo modo que la incertidumbre técnica no debe ocultarse detrás de una respuesta categórica.

Constancia de emisión Registrar qué comunicación reconoce la fuente como propia.	Preservación Conservar evidencia durable de la versión de referencia.
Verificación Permitir que terceros comprueben la atribución con baja fricción.	Deslinde verificable Demostrar que una versión alterada o fabricada no fue emitida por la fuente.

Figura 3. Dimensiones funcionales del derecho a la autenticidad de la información.

El valor del derecho no consiste en garantizar que nadie intentará falsificar. Las instituciones rara vez eliminan por completo las conductas que regulan. Su propósito es reducir el éxito del engaño, disminuir los costos de verificación y devolver a la fuente legítima una capacidad demostrativa que hoy suele llegar demasiado tarde.

9. De la certeza sobre la propiedad a la certeza sobre la atribución

¿Puede la economía digital prosperar sin saber con suficiente certeza quién dijo qué?

La analogía con los derechos de propiedad es poderosa, pero exige precisión. La información no es idéntica a una parcela, una casa o una máquina; las ideas pueden compartirse sin que su poseedor original deje de utilizarlas; y la libertad de expresión impone límites a cualquier pretensión de control total sobre el lenguaje.

Por la misma razón, hablar de “derecho a las propias palabras” no significa atribuir al emisor un dominio perpetuo sobre toda cita, interpretación o transformación. Significa reconocer un interés legítimo en que la atribución del mensaje original pueda ser establecida y controvertida mediante evidencia.

La analogía no reside en afirmar que toda palabra debe ser apropiable. Reside en las funciones institucionales. Los derechos de propiedad permiten atribuir, registrar, transferir, defender y resolver disputas sobre determinados bienes. Reducen incertidumbre sobre quién puede hacer qué y sobre qué base.

La autenticidad informativa necesita capacidades funcionalmente semejantes: atribuir una comunicación; registrar su versión de origen; preservar evidencia; verificar la correspondencia de una copia; identificar alteraciones; y resolver disputas cuando existen errores, compromisos de claves o reclamaciones contrapuestas.

Así como el desarrollo económico necesitó instituciones que redujeran la incertidumbre sobre quién era dueño de qué, la economía digital necesita instituciones que reduzcan la incertidumbre sobre quién dijo qué.

Esta formulación no pretende convertir todas las comunicaciones en propiedad exclusiva. Busca proteger la atribución. Una persona puede citar, criticar o transformar un discurso, pero no debería poder presentar la transformación como si fuera el discurso original. Una plataforma puede alojar contenido, pero no debería ser la única autoridad capaz de demostrar su origen. Una institución puede corregir un comunicado, pero la historia de las versiones debe permanecer verificable.

El derecho a la autenticidad complementa, por tanto, al derecho de autor, a la firma electrónica, a la protección de identidad, al derecho de réplica y a las reglas de evidencia. Cada uno protege una dimensión diferente. La aportación específica consiste en hacer verificable, para el público ordinario y a escala de Internet, la continuidad entre la fuente y la versión que circula.

10. Los costos sociales y económicos de la inautenticidad

¿Cuándo una falsificación digital deja de ser intangible?

Una falsificación parece intangible hasta que alguien actúa a partir de ella. Un audio apócrifo puede provocar una transferencia fraudulenta; un comunicado falso puede afectar una cotización; una alerta sanitaria manipulada puede desalentar una vacunación; una orden de evacuación falsa puede generar pánico; un video atribuido a un candidato puede alterar preferencias electorales.

El primer costo es la incertidumbre. Cuando los receptores no pueden establecer con rapidez si una comunicación es auténtica, deben invertir tiempo, conocimientos y recursos en verificarla. Cada mensaje crítico genera costos de búsqueda, confirmación y coordinación. Las instituciones deben activar equipos de crisis; los medios deben localizar fuentes; los ciudadanos deben decidir si esperar o actuar.

El segundo costo es la velocidad asimétrica. La falsificación puede distribuirse en segundos; la aclaración suele requerir encontrar el contenido, analizarlo, obtener autorización y alcanzar a una audiencia que ya se fragmentó. La corrección rara vez sigue el mismo camino ni genera la misma atención emocional que el engaño inicial.

El tercer costo es la erosión generalizada de confianza. Cuando el público aprende que cualquier imagen, audio o documento puede ser falsificado, surge el llamado “dividendo del mentiroso”: incluso el contenido auténtico puede ser negado como artificial. La crisis deja de consistir solamente en creer lo falso; también consiste en dejar de creer lo verdadero.

En los mercados, esta dinámica puede producir “corridas de confianza”. La teoría económica sobre corridas bancarias mostró cómo expectativas y rumores pueden coordinar comportamientos que terminan materializando una crisis. En la economía digital, una comunicación atribuida a una empresa, un banco central o una autoridad puede desencadenar decisiones antes de que exista tiempo para verificarla.⁵

Una infraestructura de autenticidad puede reducir estos costos al ofrecer un punto de referencia temprano. No elimina el juicio ni garantiza obediencia, pero acorta el camino entre la duda y la evidencia. En situaciones donde minutos importan, esa reducción puede tener valor económico y social significativo.

11. Gobiernos, servicios públicos y comunicación institucional

¿Qué ocurre cuando se falsifica la voz de una institución que sirve a millones?

Pocas organizaciones hablan, de manera cotidiana, con audiencias tan amplias como los gobiernos. Y su papel no se limita a seguridad, defensa, recaudación o regulación. En numerosos países, las instituciones públicas constituyen la columna vertebral de la salud, la educación, la protección social, la investigación científica, la cultura, la información y la infraestructura económica.

Los Estados operan hospitales, centros de salud, laboratorios, campañas de vacunación, escuelas, universidades, sistemas de becas, registros civiles, tribunales, bancos centrales, autoridades fiscales, redes de transporte, sistemas de protección civil, servicios meteorológicos, medios públicos, canales de televisión y agencias nacionales de noticias. Cada una de estas instituciones comunica instrucciones, decisiones y datos que pueden afectar a millones de personas.

Además, los gobiernos trasladan cada vez más trámites y servicios a Internet. Identidad digital, declaraciones fiscales, expedientes, citas médicas, inscripciones escolares, licencias, pagos, alertas y consultas se realizan mediante plataformas digitales. La autenticidad de la comunicación deja de ser un asunto de imagen institucional y se convierte en una condición de continuidad operativa y acceso a derechos.

Un comunicado falso de salud pública puede modificar conductas sanitarias; una convocatoria educativa apócrifa puede defraudar a familias; una alerta de emergencia manipulada puede poner vidas en riesgo; una circular falsa de un regulador puede afectar mercados; una noticia fabricada y atribuida a un medio público puede amplificarse con la legitimidad del Estado.

Los gobiernos ya operan una parte creciente de su actividad en la dimensión 4.5. Por ello, “hacer que la confianza sea nativa de Internet” no es una aspiración abstracta: significa dotar a los servicios públicos digitales de mecanismos de procedencia, integridad y verificación equivalentes a los registros, sellos y formalidades que durante siglos sostuvieron la actuación pública en el mundo físico.

La infraestructura debe, sin embargo, diseñarse para no confundir autenticidad gubernamental con verdad gubernamental. Los ciudadanos deben poder demostrar que un comunicado provino de una autoridad, y conservar intacto su derecho a cuestionarlo. La verificación fortalece la rendición de cuentas precisamente porque fija qué fue lo que la institución dijo en un momento determinado.

12. Democracia, elecciones y esfera pública

¿Puede existir deliberación democrática cuando la atribución de las palabras es incierta?

La democracia exige saber quién sostuvo qué posición. Los ciudadanos evalúan a candidatos y gobiernos por lo que dicen y hacen; los partidos compiten mediante propuestas; las autoridades electorales comunican reglas, fechas y resultados; los medios documentan declaraciones y hechos.

La manipulación de estas comunicaciones puede distorsionar la deliberación antes de que un voto sea emitido. Un video alterado puede atribuir a un candidato una posición que nunca sostuvo; un audio sintético puede fabricar una confesión; una falsa instrucción electoral puede desalentar la participación; un comunicado apócrifo puede sembrar dudas sobre un resultado.

Hannah Arendt destacó el papel de la palabra y la acción en la esfera pública; Habermas vinculó la legitimidad democrática con procesos de deliberación en los que los participantes pueden formular y discutir pretensiones de validez. La autenticidad no garantiza una deliberación racional, pero su ausencia vuelve más difícil incluso saber quién participa y qué posición defendió realmente.⁶

El derecho a la autenticidad no debe utilizarse para privilegiar voces oficiales sobre voces disidentes. Una democracia necesita anonimato legítimo, periodismo de investigación, sátira, filtraciones de interés público y protección de denunciantes. La arquitectura debe distinguir entre ocultar la identidad para protegerse y suplantar la identidad de otro para engañar.

La contribución específica de una infraestructura de autenticidad electoral sería permitir que los candidatos, partidos, autoridades y medios establezcan versiones verificables de sus comunicaciones, y que los ciudadanos consulten esas referencias mediante canales de uso cotidiano. No resolvería por sí sola la polarización o la propaganda, pero reduciría una forma particularmente corrosiva de manipulación: atribuir exitosamente a otro palabras que nunca pronunció.

Una esfera pública que no puede reconocer la autoría de sus mensajes pierde la base mínima para asignar responsabilidad. Y sin responsabilidad atribuible, la libertad de expresión corre el riesgo de convertirse en libertad para hablar con la identidad ajena.

13. La institución pendiente de la economía digital

¿Qué pieza falta todavía en la arquitectura institucional de Internet?

Reconocer el problema obliga a pensar en una institución, no en una sola herramienta. La solución no puede depender de una plataforma, de una empresa generadora de inteligencia artificial o de una autoridad central que determine la verdad. Tampoco puede reducirse a un algoritmo de detección: toda técnica probabilística comete errores y toda señal puede desaparecer al cambiar de formato.

La institución pendiente debe concebirse como un ecosistema de capacidades interoperables: identidad legítima del emisor, registro de origen, evidencia criptográfica, procedencia, verificación universal, detección de alteraciones, gobernanza, auditoría y mecanismos de corrección.

Los estándares de procedencia como C2PA y las credenciales de contenido constituyen avances importantes. Los sistemas de marcas de agua de proveedores de IA también aportan señales útiles. Pero la vida real del contenido ocurre fuera de los entornos ideales: archivos reenviados por mensajería, capturas, documentos impresos y escaneados, recortes, traducciones, clips y recompressiones. La institución debe integrar señales múltiples y seguir funcionando cuando algunas de ellas se pierden.⁷

La institución tampoco debe confundirse con una base de datos única. Un modelo sano debería permitir registros plurales que compartan estándares, mecanismos de confianza y procesos de resolución. La neutralidad y la interoperabilidad son indispensables para que la autenticidad no dependa de la plataforma donde se creó o publicó el contenido.

La aspiración puede resumirse en una idea: que verificar la procedencia de una comunicación digital llegue a ser tan normal como comprobar la conexión segura de un sitio web. No porque ambos problemas sean técnicamente idénticos, sino porque la confianza funciona mejor cuando está integrada al uso ordinario y no reservada a especialistas.

14. Principios de una infraestructura de autenticidad

¿Qué capacidades debe combinar una infraestructura confiable?

Una infraestructura de autenticidad a escala de Internet puede entenderse mediante seis componentes y varias propiedades transversales.

1. Identidad legítima del emisor

El sistema debe establecer quién está autorizado para registrar contenido en nombre de una persona u organización. En instituciones complejas, la identidad no basta: también se requieren roles, delegaciones, separación de funciones, vigencia y revocación.

2. Registro de origen

La fuente debe poder declarar y registrar una versión de referencia antes o al momento de publicar, con fecha, contexto y metadatos suficientes. Esa condición de referencia acredita qué versión reconoce la fuente como emitida; no la convierte en verdadera ni jurídicamente superior a toda evidencia posterior. El registro no tiene que almacenar siempre el contenido completo: puede conservar huellas y referencias bajo reglas de privacidad y retención.

3. Evidencia criptográfica

Firmas digitales, funciones hash, sellos de tiempo y registros resistentes a alteraciones deben combinarse para corroborar la integridad, la autoría técnica y la secuencia temporal de la evidencia. Ninguno de estos elementos, utilizado aisladamente, resuelve toda la cadena de confianza. La seguridad debe incluir custodia de claves, módulos de hardware, recuperación, rotación, revocación y respuesta a compromisos.

4. Verificación universal

La evidencia pierde gran parte de su valor si el ciudadano común no puede utilizarla. La verificación debe estar disponible mediante web, APIs y canales de mensajería, idealmente sin pago, sin conocimientos especializados y sin exigir un perfil de usuario.

5. Detección de alteraciones

Cuando el contenido no coincide exactamente, técnicas de hashing perceptual, fingerprints, análisis forense, modelos de similitud y detección multimodal pueden identificar relaciones con un original. Sus resultados deben expresar incertidumbre y estar sujetos a evaluación adversarial.

6. Gobernanza y debido proceso

Deben existir procedimientos para correcciones, revocaciones, disputas, cambios de gobierno, fusiones, desaparición de instituciones y compromiso de credenciales. Una infraestructura confiable necesita reglas tan sólidas como sus algoritmos.

Propiedades transversales

- Interoperabilidad y apertura: APIs documentadas, estándares abiertos y portabilidad.
- Privacidad por diseño: minimización de datos y verificación sin vigilancia innecesaria.
- Accesibilidad: idiomas, discapacidad, conectividad limitada y alfabetización digital diversa.
- Agilidad criptográfica: capacidad para cambiar algoritmos sin invalidar todo el sistema.
- Resiliencia poscuántica: adopción progresiva de estándares NIST según su función —por ejemplo, ML-DSA o SLH-DSA para firmas y ML-KEM para establecimiento de claves cuando exista confidencialidad—, junto con estrategias de transición, renovación y coexistencia criptográfica. El objetivo es reducir riesgos futuros de falsificación de firmas y de exposición retrospectiva de información protegida.⁸
- Preservación de largo plazo: renovación de attestaciones, archivos auditables y continuidad institucional.

La combinación de estos elementos debe evitar una ilusión común: creer que una herramienta única resolverá un problema institucional. La autenticidad es una cadena. Basta que falle la identidad, la custodia de claves, la interfaz de verificación o la gobernanza para que la confianza se deteriore.

1. Identidad legítima Vincula a la fuente con una autoridad reconocible.	2. Registro de origen Conserva una versión de referencia y su contexto.
3. Evidencia criptográfica Protege integridad, firma y temporalidad.	4. Verificación universal Permite consultar autenticidad con baja fricción.
5. Detección de alteraciones Relaciona versiones modificadas con sus referentes.	6. Gobernanza y debido proceso Corrige errores, resuelve disputas y limita abusos.

Figura 4. Componentes de una infraestructura de autenticidad.

Propiedades transversales: interoperabilidad · privacidad · accesibilidad · agilidad criptográfica · resiliencia poscuántica

15. Riesgos, salvaguardas y límites

¿Cómo construir confianza sin crear censura, vigilancia o concentración de poder?

Toda infraestructura de confianza contiene, también, una posibilidad de poder. Por ello, sus salvaguardas no deben añadirse al final: deben formar parte de la arquitectura desde el inicio.

No convertirse en censura

El sistema debe acreditar procedencia, no decidir qué ideas pueden circular. Un contenido no registrado debe poder existir y expresarse. La etiqueta “no encontrado” no puede convertirse en sinónimo de falso o prohibido.

No crear una autoridad universal de la verdad

Ninguna empresa, gobierno o plataforma debe tener monopolio sobre la verdad. Los registros deben ser plurales, auditables e interoperables. La autenticidad técnica no debe desplazar el juicio humano, la investigación o el debate.

Proteger anonimato y libertad de expresión

La protección de la atribución no implica exigir identidad pública a todos. Periodistas, denunciantes, víctimas y disidentes pueden necesitar anonimato. El sistema debe impedir la suplantación sin convertir toda expresión en comunicación obligatoriamente identificada.

Minimizar datos personales

La verificación pública no debe convertirse en un mecanismo para perfilar quién consulta qué. Deben evitarse la recopilación innecesaria de identidad, ubicación, contactos o comportamiento de los verificadores.

Expresar incertidumbre

Los sistemas de detección deben distinguir coincidencia exacta, similitud, alteración probable, ausencia de referencia y evidencia insuficiente. La humildad conceptual es una salvaguarda: un resultado técnico nunca equivale a omnisciencia.

Garantizar corrección y apelación

Una fuente puede registrar por error, una clave puede ser robada y una institución puede cambiar de autoridades. Deben existir procedimientos de revocación, corrección, auditoría, trazabilidad y resolución de disputas.

Evitar exclusión estructural

Si solo las grandes organizaciones pueden certificar, la infraestructura reproducirá desigualdades. Deben existir mecanismos proporcionados para individuos, pequeñas empresas, comunidades, medios locales y organizaciones de la sociedad civil.

La meta no es un Internet en el que todo deba ser certificado. Es un Internet en el que las fuentes legítimas puedan demostrar lo que emitieron, y las personas puedan verificarlo cuando las consecuencias lo justifiquen.

16. AliPsé como hipótesis de implementación

¿Cómo puede una idea institucional convertirse en una experiencia sencilla y útil?

AliPsé nació de la intuición que abre este ensayo: las personas y las instituciones deberían conservar el derecho práctico a sus propias palabras en la dimensión digital. Su aspiración es materializar esa idea mediante una infraestructura abierta y agnóstica respecto de las herramientas utilizadas para crear contenido.

La hipótesis es deliberadamente sencilla. Combina cuatro capacidades: un registro de contenidos auténticos; certificación al origen; verificación pública de baja fricción; y una capa de inteligencia capaz de identificar alteraciones o relaciones con versiones registradas. Los clientes institucionales registrarían —“AliPsellarían”— sus comunicaciones antes de publicarlas; los usuarios podrían “Alipsear” un contenido y consultar si coincide con una referencia auténtica.

El modelo distingue entre quien financia y quien verifica. Las organizaciones pagan por servicios de registro, certificación, integración y cumplimiento; la verificación pública debe ser gratuita y, cuando sea posible, no requerir inicio de sesión. Esta estructura busca reducir los costos de transacción y favorecer un efecto de red: cada contenido auténtico registrado aumenta la utilidad del sistema para todos los verificadores.

AliPsé no pretende reemplazar C2PA, Content Credentials, SynthID, OpenAI Verify u otras tecnologías. Las considera señales que pueden integrarse en una arquitectura más amplia. La pregunta de AliPsé no es únicamente “¿qué herramienta produjo esto?”, sino “¿corresponde este contenido a una versión que la fuente legítima registró o reconoció como propia?”.

La propuesta debe evaluarse con rigor. Será necesario demostrar precisión, resistencia adversarial, adopción institucional, utilidad ciudadana, sostenibilidad económica, protección de derechos y gobernanza independiente. AliPsé es una hipótesis de implementación, no la única forma posible de construir la institución descrita en este documento.

La autenticidad de la información es demasiado importante para pertenecer exclusivamente a una empresa, una plataforma o un gobierno. Si llega a convertirse en una capacidad nativa de Internet, deberá apoyarse en estándares abiertos, competencia, cooperación y mecanismos de control suficientes para sobrevivir a cualquiera de sus participantes.

Estándares y señales C2PA · Content Credentials · firmas · marcas de agua	Fuentes legítimas Personas · gobiernos · medios · empresas	Canales de distribución Web · redes sociales · mensajería · APIs
Registro y verificación AliPsé y otros servicios interoperables	Usuarios y audiencias Ciudadanos · clientes · periodistas · autoridades	Gobernanza Auditoría · competencia · corrección · debido proceso
La confianza digital no depende de una sola tecnología: emerge de un ecosistema plural, interoperable y verificable.		

Figura 5. Ecosistema abierto de autenticidad y confianza digital.

Conclusión

¿Quién protegerá nuestras palabras?

Durante siglos, las sociedades construyeron instituciones para proteger la propiedad, hacer exigibles los contratos, preservar la identidad, estabilizar la moneda y registrar los actos jurídicos. No porque esas instituciones eliminaran toda disputa, sino porque sin ellas la incertidumbre hacía más difícil cooperar, invertir, gobernar y proyectar el futuro.

Hoy, una parte creciente de la existencia humana transcurre en la dimensión digital. Allí trabajamos, aprendemos, amamos, comerciamos, gobernamos, deliberamos y conservamos memoria. Internet amplificó como nunca antes la voz humana, pero dejó sin resolver una vulnerabilidad elemental: separar las palabras de quien las emitió, alterarlas y devolverlas al mundo con apariencia de autenticidad.

La inteligencia artificial ha vuelto más urgente esa carencia, pero no la creó. El problema comenzó cuando obtuvimos la capacidad de comunicarnos globalmente sin construir, al mismo tiempo, una capacidad universal para demostrar quién dijo qué.

Las palabras no son simples caracteres. Transportan ideas, compromisos, conocimientos y decisiones. Mediante ellas las personas participan en la sociedad y las instituciones coordinan la vida colectiva. Proteger su autenticidad no significa inmunizar cada afirmación frente a la crítica; significa preservar la posibilidad de atribuirla correctamente.

Si la cooperación es uno de los grandes poderes de nuestra especie, y si esa cooperación depende de la comunicación y de la confianza, entonces la autenticidad de la información pertenece a la infraestructura simbólica que permite a la civilización continuar existiendo y prosperando.

La pregunta que queda planteada es:

¿Qué institución permitirá que las personas y las organizaciones conserven, en la economía digital, el derecho a sus propias palabras?

Este ensayo sostiene que esa institución todavía está pendiente.

Y que ha llegado el momento de comenzar a construirla.

Notas y referencias

1. Yuval Noah Harari, "Cognitive Revolution — Power and Imagination", sitio oficial del autor; véase también *Sapiens: De animales a dioses*. La tesis es influyente y útil como marco interpretativo, aunque no debe tratarse como una explicación antropológica única o incontrovertible.
2. Douglass C. North, "Economic Performance Through Time", Nobel Lecture, 1993; la presentación del Premio Nobel subrayó el papel de las instituciones para reducir incertidumbre y crear estructuras relativamente estables para la actividad humana.
3. Zygmunt Bauman, *Liquid Modernity*, Polity Press, 2000; y *Liquid Love: On the Frailty of Human Bonds*, Polity Press, 2003. El ensayo utiliza la metáfora como contexto cultural, no como explicación causal suficiente del problema de autenticidad.
4. Ludwig Wittgenstein, *Tractatus Logico-Philosophicus*, proposición 5.6; Hannah Arendt, *The Human Condition*, 1958; Jürgen Habermas, *The Theory of Communicative Action*, 1981. Estas referencias no constituyen el eje del ensayo, pero muestran la profundidad filosófica de la relación entre lenguaje, identidad pública y cooperación.
5. Douglas W. Diamond y Philip H. Dybvig desarrollaron el modelo clásico de corridas bancarias; junto con Ben S. Bernanke recibieron el Premio en Ciencias Económicas 2022 por sus investigaciones sobre bancos y crisis financieras. La analogía con "corridas de confianza" es conceptual y se propone aquí como línea de investigación, no como equivalencia formal.
6. Véanse Hannah Arendt, *The Human Condition*, y Jürgen Habermas, *Between Facts and Norms*, así como la entrada de la Stanford Encyclopedia of Philosophy sobre Habermas. Estas referencias aportan contexto teórico a la relación entre comunicación y legitimidad democrática.
7. Coalition for Content Provenance and Authenticity (C2PA), especificaciones y materiales de Content Credentials. El estándar busca conservar información verificable sobre origen y transformaciones, pero no pretende determinar la verdad de un contenido.
8. National Institute of Standards and Technology, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA), publicados en 2024. ML-KEM es un mecanismo de encapsulación de claves; ML-DSA y SLH-DSA son esquemas de firma. La estrategia adecuada no consiste en fijar un algoritmo para siempre, sino en diseñar agilidad criptográfica, coexistencia durante la transición y renovación periódica de evidencias.

Bibliografía y fuentes institucionales seleccionadas

- ARENDT, Hannah. *The Human Condition*. University of Chicago Press, 1958.
- BAUMAN, Zygmunt. *Liquid Modernity*. Polity Press, 2000.
- BAUMAN, Zygmunt. *Liquid Love: On the Frailty of Human Bonds*. Polity Press, 2003.
- COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY (C2PA). C2PA Technical Specification, versión 2.4, y materiales explicativos sobre Content Credentials. <https://c2pa.org/> y <https://spec.c2pa.org/>
- DIAMOND, Douglas W.; DYBVIG, Philip H. "Bank Runs, Deposit Insurance, and Liquidity". *Journal of Political Economy*, 1983.
- HABERMAS, Jürgen. *The Theory of Communicative Action*. Beacon Press, 1984/1987.
- HABERMAS, Jürgen. *Between Facts and Norms*. MIT Press, 1996.
- HARARI, Yuval Noah. *Sapiens: De animales a dioses*. Debate, varias ediciones.
- HARARI, Yuval Noah. "Cognitive Revolution — Power and Imagination". Sitio oficial del autor. <https://www.ynharari.com/topic/power-and-imagination/>
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204, Module-Lattice-Based Digital Signature Standard; y FIPS 205, Stateless Hash-Based Digital Signature Standard. 13 de agosto de 2024. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- NORTH, Douglass C. *Institutions, Institutional Change and Economic Performance*. Cambridge University Press, 1990.
- NORTH, Douglass C. "Economic Performance Through Time". Nobel Lecture, 1993. <https://www.nobelprize.org/prizes/economic-sciences/1993/north/lecture/>
- ORGANIZACIÓN DE LAS NACIONES UNIDAS. Our Common Agenda Policy Brief 8: Information Integrity on Digital Platforms. EOSG/2023/8, 2023.
- PROGRAMA DE LAS NACIONES UNIDAS PARA EL DESARROLLO. Information Integrity: Forging a Pathway to Truth, Resilience and Trust. Strategic Guidance, 2022.
- RODRÍGUEZ ALEMÁN, Luis Angel. "La informática en un mundo interdisciplinario". En: Reflexiones de la Academia Mexicana de Informática a los 40 años de su fundación. Universidad de Guadalajara, octubre de 2016.
- UNESCO. Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multistakeholder Approach. París, 2023.
- WITTGENSTEIN, Ludwig. *Tractatus Logico-Philosophicus*. 1921/1922.
- WORLD ECONOMIC FORUM. The Global Risks Report 2025, 20th Edition; y The Global Risks Report 2026, 21st Edition. Ginebra, 2025 y 2026.
- WORLD INTELLECTUAL PROPERTY ORGANIZATION. Copyright and Related Rights y recursos institucionales sobre derechos de autor. <https://www.wipo.int/copyright/>
- WORLD BANK GROUP. Digital Public Infrastructure and Development. Digital Public Infrastructure Policy Note Series, Washington, D.C., 2025; y recursos sobre Digital Public Infrastructure and Services.

Sobre el autor

Luis Ángel Rodríguez Alemán es ingeniero en Computación por el ITAM, maestro en Políticas Públicas por Georgetown University y maestro en Planeación Regional y Urbana por la London School of Economics. Ha ocupado responsabilidades de alta dirección tecnológica en banca, gobierno y educación, y es miembro numerario de la Academia Mexicana de Informática (AMIAC), del CIO Club, de CISO Club y de CIOs LATAM. Es fundador de AliPsé, iniciativa orientada a construir infraestructura de confianza para contenidos digitales.

Contacto: luisangel@alipse.net · www.alipse.net

Aviso: este documento es un ensayo conceptual y de política pública. No constituye asesoría jurídica, estándar técnico ni afirmación de que el derecho propuesto se encuentre reconocido actualmente en una jurisdicción determinada.