REPÚBLICA DE COSTA RICA
ASAMBLEA LEGISLATIVA

PROYECTO DE LEY

LEY MARCO DE SOBERANÍA DIGITAL Y TECNOLOGÍAS EMERGENTES DE COSTA RICA

ARQUITECTURA NACIONAL PARA LOS DERECHOS DIGITALES, LOS ACTIVOS DIGITALES, BLOCKCHAIN, INTELIGENCIA ARTIFICIAL Y LA SOBERANÍA TECNOLÓGICA

Marco fundacional de Estado para una democracia digital garantista, una industria Web3 competitiva, infraestructura pública verificable y protección de las libertades del siglo XXI.

Arquitectura Legal del Proyecto: Stephanie Sánchez | MissCryptoLawyer®

BlockRock Legal & Tech

San José, Costa Rica
Septiembre de 2026 | Versión legislativa V5

EXPOSICIÓN DE MOTIVOS

I. Objeto y decisión de Estado

Costa Rica enfrenta una decisión generacional: limitarse a recibir las reglas digitales diseñadas por otras jurisdicciones o construir una arquitectura jurídica propia que proteja la libertad, otorgue certeza a la innovación y preserve la soberanía tecnológica. La transformación digital ya afecta la identidad, la propiedad, el comercio, los mercados, la educación, la administración pública, la inteligencia artificial y la infraestructura que sostiene los derechos fundamentales. Esta ley propone una respuesta integral y de largo plazo.

La iniciativa se concibe como ley marco. Su función es establecer principios, derechos, perímetros regulatorios, instituciones, deberes de interoperabilidad, reglas de protección al usuario y mecanismos de transición que puedan ser desarrollados técnicamente sin convertir la legislación en una descripción estática de tecnologías particulares.

II. Una vía costarricense: constitucionalmente garantista y tecnológicamente neutral

El propósito no es copiar MiCA, El Salvador, Dubái, Suiza, Singapur, Hong Kong, Wyoming ni ningún otro sistema. El derecho comparado sirve como referencia, pero el modelo costarricense se diferencia por colocar los derechos digitales y los límites al poder tecnológico en el centro de la arquitectura regulatoria. Costa Rica aspira a consolidarse como una jurisdicción Web3 constitucionalmente garantista, capaz de combinar innovación, seguridad jurídica, integridad de mercado, cumplimiento internacional y libertades fundamentales.

El principio rector es sencillo: la libertad no desaparece cuando la vida se traslada al entorno digital. La identidad digital, la privacidad, la propiedad, el debido proceso, la libertad de expresión, la libertad contractual y la autonomía personal deben conservar protección efectiva también cuando se ejercen mediante criptografía, software, wallets, redes distribuidas, datos, inteligencia artificial y activos digitales.

III. Derechos y garantías digitales del siglo XXI

La ley reconoce y desarrolla, dentro del marco constitucional vigente, la identidad digital soberana, la autodeterminación informativa, la privacidad digital y financiera, la propiedad digital, la autocustodia, el uso legítimo de criptografía, el pseudonimato legítimo, la portabilidad, la interoperabilidad y el debido proceso algorítmico. La publicación y desarrollo de código abierto se protege como actividad lícita vinculada a la libertad de expresión, la investigación, la innovación y la creación intelectual, sin eximir de responsabilidad a quien utilice el software para ejecutar o controlar conductas ilícitas.

Se establecen límites frente a vigilancia digital masiva, scoring social, debilitamiento obligatorio del cifrado, puertas traseras generalizadas, identidad digital universal coercitiva, censura financiera arbitraria y decisiones automatizadas irrevisables. La regulación de inteligencia artificial se estructura según riesgo y efecto sobre derechos, con especial rigor para sistemas públicos o privados de alto impacto.

IV. Libertad financiera, autocustodia y arquitectura abierta

La autocustodia se reconoce como manifestación contemporánea del derecho de propiedad: quien mantiene control exclusivo de sus llaves y de sus activos propios no se convierte por ese hecho en intermediario financiero. La regulación se dirige a la prestación profesional de servicios a terceros, al control efectivo, a la custodia ajena, a la emisión, a la intermediación, al fraude y a los riesgos de mercado.

La ley distingue entre Bitcoin y otros activos digitales descentralizados sin emisor; stablecoins; tokens de pago, utilidad, gobernanza o inversión; activos tokenizados del mundo real; NFTs; activos sintéticos; infraestructura DeFi y demás categorías funcionales. La clasificación sigue la sustancia económica, los derechos incorporados y el grado de control efectivo, no el nombre comercial ni la tecnología utilizada.

V. IID: regulación especializada dentro del MICITT con desconcentración máxima

Se crea la Intendencia de la Industria Descentralizada (IID) como órgano especializado de desconcentración máxima adscrito al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), con independencia técnica, funcional, administrativa y de gestión presupuestaria en las materias expresamente desconcentradas por esta ley. La IID forma parte de la Administración Central; no constituye una institución autónoma ni un ente público separado del Estado. Su adscripción al ministerio rector de ciencia, innovación y tecnología permite integrar la política pública nacional con una regulación sectorial especializada, sin someter las decisiones regulatorias concretas a dirección jerárquica.

La IID tendrá competencia sectorial primaria sobre activos digitales, proveedores de servicios de activos digitales, mercados digitales nativos —centralizados o descentralizados—, emisiones y valores digitales nativos, tokenización, RWA, stablecoins dentro del ámbito no monetario, DAOs reguladas y demás actividades definidas por esta ley. Las competencias monetarias del Banco Central de Costa Rica, las prudenciales de la supervisión bancaria, las obligaciones AML/CFT y las competencias constitucionales o legales exclusivas de otros órganos se preservan expresamente. Los productos híbridos se resolverán mediante reglas de perímetro y coordinación, evitando duplicidad regulatoria.

El diseño utiliza la desconcentración máxima como técnica de distribución de competencias dentro de la Administración Central. En las materias legalmente desconcentradas, el jerarca ministerial no podrá avocar competencias de la IID, revisar o sustituir sus decisiones ni impartir órdenes, instrucciones o circulares sobre la forma de resolver asuntos concretos. La IID podrá contar con personalidad jurídica instrumental únicamente para actividad contractual, administración de los recursos que legalmente le correspondan y celebración de convenios, sin que ello la convierta en una institución autónoma. Su presupuesto se individualizará dentro del Presupuesto Nacional y quedará sujeto al Ministerio de Hacienda, al control interno, a la fiscalización de la Contraloría General de la República y al ordenamiento financiero aplicable.

La rectoría política nacional en ciencia, innovación, tecnología, transformación digital y materias afines permanecerá en el MICITT. La IID ejercerá las competencias regulatorias, supervisoras, autorizatorias, fiscalizadoras y sancionatorias que esta ley desconcentra expresamente, con independencia decisoria y sujeción al debido proceso, al control judicial y a los mecanismos de rendición de cuentas. La presente ley incorpora, además, las reformas de armonización necesarias a la Ley N.° 7169 para hacer explícita esa distribución entre rectoría ministerial y competencia técnica desconcentrada.

VI. Infraestructura crítica digital y soberanía nacional

La ley reconoce que la soberanía digital no se agota en la regulación de mercados. Los sistemas que sostienen identidad, registros, datos públicos críticos, telecomunicaciones, pagos, salud, educación, justicia, servicios esenciales, nube estatal, inteligencia artificial pública, criptografía y otros servicios de alta relevancia constituyen infraestructura digital crítica y estratégica.

La IID ejercerá, como órgano técnico especializado del MICITT, una función transversal en soberanía digital e infraestructura crítica: inventariará riesgos; desarrollará y verificará estándares mínimos; evaluará criptografía, gestión de llaves, resiliencia, reversibilidad contractual, portabilidad, interoperabilidad, dependencia de proveedores, cadena de suministro, ciberseguridad, uso de IA, minimización de datos y criptoagilidad post-cuántica; y practicará auditorías técnicas de conformidad. Esta función no sustituye fiscalización presupuestaria, dirección electoral, jurisdicción, investigación penal, política monetaria ni otras competencias constitucionalmente exclusivas.

Toda institución pública quedará sujeta directamente por ley a los estándares mínimos de soberanía digital y protección de derechos. La IID verificará su cumplimiento técnico con respeto a la separación de poderes y autonomías constitucionales. En los órganos con competencias constitucionalmente exclusivas, las observaciones

se instrumentarán mediante informes técnicos de riesgo, planes de remediación y mecanismos de coordinación, sin avocación ni sustitución de la competencia sustantiva.

VII. Blockchain como infraestructura anticorrupción

La propuesta utiliza blockchain y otras tecnologías de registro distribuido como capa de integridad, no como sustituto automático de instituciones. Contratación pública, trazabilidad presupuestaria, registros, certificaciones, activos públicos, evidencia criptográfica y control de cambios pueden beneficiarse de mecanismos verificables, sellos de tiempo, hashes y registros inmutables o resistentes a alteración. La regla se invierte: el poder público debe ser más verificable sin convertir al ciudadano en objeto de vigilancia permanente.

VIII. Inteligencia artificial, neuroderechos e infancia digital

La inteligencia artificial se regula bajo dignidad humana, evaluación de riesgo, trazabilidad, explicabilidad proporcional, supervisión humana y posibilidad de impugnación cuando produzca efectos jurídicos o materiales relevantes. Se prohíben la vigilancia masiva y el espionaje algorítmico generalizado de la ciudadanía. La investigación individualizada, la ciberseguridad y las funciones legítimas del Estado permanecen sujetas a la ley, necesidad, proporcionalidad y debido proceso.

La ley incorpora protección reforzada de neurodatos, libertad cognitiva, integridad mental y continuidad psicológica, así como un régimen especial para niños, niñas y adolescentes frente a explotación de datos, manipulación algorítmica, diseño adictivo y sistemas de IA de alto impacto.

IX. Dinero digital y límites democráticos

La propuesta no impide la modernización monetaria ni la innovación de pagos. Prohíbe, en cambio, que una moneda digital estatal minorista se imponga coercitivamente o se diseñe como infraestructura de vigilancia masiva, scoring social, expiración arbitraria, restricción conductual generalizada o censura económica política. La innovación monetaria pública debe respetar privacidad, libertad de elección, debido proceso y las competencias constitucionales del Banco Central.

X. Competitividad, inversión y cooperación internacional

Costa Rica puede convertir su estabilidad institucional, Estado de Derecho, talento humano, matriz energética, sistema de zonas francas y tradición democrática en una ventaja competitiva para atraer infraestructura Web3, tokenización, activos digitales, centros de datos, ciberseguridad, IA auditable, servicios de cumplimiento, arbitraje digital y exportación de servicios tecnológicos. La cooperación con GAFI, OCDE y otros organismos deberá seguir un enfoque basado en riesgo sin criminalizar autocustodia, código abierto o interacción peer-to-peer lícita.

XI. Unidad legislativa y desarrollo constitucional complementario

La ley se presenta como un marco legislativo integral patrocinable por la Asamblea Legislativa. Las normas ordinarias, regulatorias, institucionales, administrativas, fiscales y penales que integran este cuerpo deben tramitarse con las mayorías y consultas que correspondan. Las nuevas garantías que se pretenda incorporar literalmente al texto de la Constitución Política deberán, por mandato constitucional, tramitarse mediante el procedimiento especial de reforma parcial. Ambas piezas forman una sola arquitectura política de soberanía digital, aunque jurídicamente utilicen los vehículos exigidos por la Constitución.

XII. Visión regional

Costa Rica no necesita ser el país que más controle la economía digital; necesita ser el país que mejor comprenda qué debe proteger, qué debe supervisar y qué no debe capturar. La ambición de esta ley es ofrecer a América Latina un modelo replicable: regulación especializada, límites al poder digital, derechos efectivos, infraestructura resiliente,

mercados abiertos, protección del usuario, responsabilidad según control efectivo y una institucionalidad capaz de evolucionar con la tecnología.

El objetivo final es que Costa Rica no llegue tarde al futuro digital, sino que contribuya a diseñarlo desde su propia tradición constitucional, democrática y humanista.

GLOSARIO Y DEFINICIONES GENERALES

Para efectos de interpretación inicial del presente proyecto de ley, se entenderán los siguientes conceptos sin perjuicio de las definiciones específicas que cada capítulo pueda desarrollar:

Jurisdicción / marco	Elemento relevante	Aplicación al proyecto	Diferenciador costarricense
MiCA - Unión Europea	Licenciamiento CASP, stablecoins y protección de mercado.	Base útil para supervisión institucional.	Evitar rigidez excesiva y proteger autocustodia.
UAE / VARA	Regulador especializado y enfoque pro-innovación.	Inspiración para regulación especializada e IID.	Reforzar garantías constitucionales y transparencia.
Hong Kong	Regulación de plataformas, custodia, mercados y stablecoins.	Modelo de integración financiera institucional.	Evitar concentración excesiva y proteger derechos.
Singapur	Supervisión rigurosa, innovación controlada y reputación financiera.	Referencia para AML/KYT, sandbox y estabilidad.	No sacrificar apertura legítima de tecnologías descentralizadas.
El Salvador	Marco digital, Bitcoin, DASP y atracción de industria.	Competidor regional directo.	Diferenciarse por democracia digital, DEPA, IA y neuroderechos.
Wyoming	DAOs, custodia digital y estructuras jurídicas Web3.	Referencia para personalidad digital y propiedad.	Tropicalización al derecho costarricense.
Utah / SEDI	Identidad digital soberana, no phone-home y credenciales.	Fortalece SSI y privacidad operativa.	Elevarlo a estándar constitucional.
Chile neuroderechos	Protección constitucional de la mente y neurodatos.	Referencia pionera en neuroderechos.	Integrarlo con IA, datos e infancia digital.
DEPA	Interoperabilidad, comercio digital, identidad, pagos y datos.	Base internacional para economía digital.	Interoperar sin perder soberanía digital.

GAFI/FATF	Recomendación 15, VASP, Travel Rule y enfoque basado en riesgo.	Necesario para legitimidad financiera global.	Cumplir sin vigilancia masiva ni prohibición de autocustodia.

Término	Definición
Activo digital	Representación digital de valor, derecho, credencial, utilidad, gobernanza, propiedad, instrumento económico o registro verificable mediante tecnología digital, blockchain o sistemas criptográficos.
Activo digital descentralizado sin emisor	Activo digital que opera en una red abierta sin emisor, administrador central, promesa de rendimiento ni control unilateral identificable. Bitcoin es el ejemplo principal.
Autocustodia	Control directo de activos digitales por la persona titular mediante llaves privadas, wallets no custodiales, hardware wallets, multisig o smart contracts.
Bitcoin	Activo digital descentralizado, sin emisor ni administrador central, basado en una red pública y verificable.
Blockchain	Tecnología de registro distribuido que permite registrar información, transacciones o eventos de forma verificable, trazable y resistente a alteración.
IID	Intendencia de la Industria Descentralizada: órgano técnico de desconcentración máxima adscrito al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), con independencia técnica y funcional en las materias legalmente desconcentradas y personalidad jurídica instrumental limitada a los fines autorizados por esta ley.
Criptografía	Conjunto de técnicas matemáticas para proteger información, identidad, comunicaciones, firmas, transacciones y activos digitales.
DAO	Organización Autónoma Descentralizada, estructura digital de coordinación y gobernanza basada en smart contracts, votación digital, tokens, multisig o reglas programables.
DeFi	Finanzas descentralizadas: protocolos o sistemas financieros ejecutados mediante smart contracts y redes blockchain, con diferentes grados de descentralización y control efectivo.

DID	Identificador descentralizado que permite representar identidad o atributos sin dependencia de un registro central único.
Fe pública criptográfica	Uso de mecanismos criptográficos para acreditar integridad, fecha, autenticidad, trazabilidad o existencia de actos, documentos o registros con valor jurídico.
Identidad digital soberana	Modelo de identidad en el cual la persona controla sus credenciales, identificadores, atributos y mecanismos de autenticación.
AML/CFT	Prevención de lavado de dinero, financiamiento del terrorismo y financiamiento de proliferación.
KYC	Know Your Customer: procedimiento de identificación y debida diligencia aplicable a sujetos obligados según riesgo y actividad.
NFT	Token no fungible que representa un activo único o individualizable, digital o vinculado a derechos específicos.
Oráculo	Sistema que introduce datos externos a un smart contract o protocolo blockchain.
Proof of Reserves	Prueba, auditoría o mecanismo verificable que acredita reservas mantenidas por una entidad frente a obligaciones o activos emitidos.
Proof of Clean Funds	Mecanismo para acreditar razonablemente que determinados fondos digitales no presentan exposición relevante a fuentes ilícitas conocidas.
RWA	Real World Assets: activos del mundo real representados digitalmente mediante tokens.
Smart contract	Código o mecanismo programable que ejecuta reglas, condiciones, transferencias u obligaciones de forma automatizada.
Stablecoin	Activo digital diseñado para mantener referencia de valor respecto de una moneda, activo, cesta, colateral o mecanismo de estabilización.
Token	Unidad digital registrada o transferible que puede representar valor, derecho, acceso, gobernanza, propiedad, identidad o función dentro de un sistema.
Tokenización	Representación digital de un activo, derecho, obligación o flujo económico mediante tokens o registros verificables.
VASP	Proveedor de servicios sobre activos virtuales o digitales que presta profesionalmente servicios

	como custodia, intercambio, transferencia, administración o intermediación de activos digitales.
Wallet no custodial	Herramienta que permite al usuario controlar directamente sus llaves privadas y activos digitales sin que un tercero custodie los fondos.
ZKP	Zero Knowledge Proof o prueba de conocimiento cero: mecanismo criptográfico que permite demostrar una condición sin revelar la información subyacente completa.
CBDC	Moneda digital de banco central. En el proyecto se prohíbe cuando sea obligatoria o diseñada para vigilancia o control social.
Debanking	Cierre, negación o restricción de servicios bancarios o financieros por razones arbitrarias o discriminatorias.
Control efectivo	Capacidad real de una persona, entidad o grupo para modificar, administrar, censurar, custodiar, bloquear, actualizar o controlar un sistema, activo, protocolo o servicio.
Neuroderechos	Derechos fundamentales destinados a proteger la libertad cognitiva, privacidad mental, integridad mental y continuidad psicológica frente a neurotecnologías, IA y sistemas de manipulación cognitiva.
Neurodatos	Datos cerebrales, neuronales, neurofisiológicos, cognitivos o inferencias mentales derivados directa o indirectamente del sistema nervioso, sujetos a protección reforzada.
Infancia digital	Conjunto de derechos y garantías de niños, niñas y adolescentes en entornos digitales, incluyendo protección contra manipulación algorítmica, explotación de datos y diseño adictivo.
Soberanía energética digital	Capacidad nacional de sostener infraestructura tecnológica crítica mediante energía segura, renovable, resiliente, distribuida y estratégicamente gestionada.
Testamento criptográfico	Disposición sucesoria o instrucción digital que regula transmisión, recuperación o administración post-mortem de activos digitales, llaves, wallets, datos o identidad digital.
Derechos digitales post-mortem	Derechos relativos a identidad digital, activos, datos, IA personal, memoria digital y reputación de una persona después de su fallecimiento.

KYT	Know Your Transaction: proceso de monitoreo y análisis de transacciones digitales, wallets, exposición ilícita, patrones de riesgo y flujos on-chain conforme a un enfoque basado en riesgo.
Infraestructura de liquidación y pagos fiat-digitales	Infraestructura operativa que conecta moneda fiduciaria, bancos, sistemas de pago, APIs financieras, stablecoins, depósitos tokenizados y liquidación on-chain.
OTC institucional	Servicios profesionales de negociación extrabursátil de activos digitales, stablecoins o activos tokenizados para clientes institucionales, con controles de liquidez, contraparte, cumplimiento y trazabilidad.
ISO 20022	Estándar internacional de mensajería financiera que facilita interoperabilidad, datos estructurados y compatibilidad entre sistemas de pagos, banca e infraestructura financiera digital.
Onboarding institucional	Proceso reforzado de incorporación de clientes o participantes institucionales mediante debida diligencia, verificación de beneficiarios finales, source of funds, source of wealth, gobernanza, ciberseguridad y controles operativos.
Tesorería digital	Gobernanza financiera y operativa de reservas, liquidez, activos digitales, stablecoins, llaves criptográficas, reconciliación, custodia, contraparte y continuidad operacional.
Tecnologías emergentes	Conjunto de tecnologías con capacidad disruptiva o estratégica, incluyendo blockchain, inteligencia artificial, computación cuántica o post-cuántica, neurotecnología, sistemas descentralizados, identidad digital, cloud soberano, automatización avanzada y tecnologías futuras análogas.
Web4	Evolución de infraestructuras digitales hacia entornos interoperables, inteligentes, descentralizados, automatizados y conectados con inteligencia artificial, identidad soberana, activos digitales y sistemas verificables.
Travel Rule	Estándar internacional aplicable a transferencias entre sujetos obligados o VASP, orientado al intercambio de información originador-beneficiario conforme a reglas AML/CFT y proporcionalidad.
IVMS101	Estándar de mensajería para interoperabilidad de información requerida por la Travel Rule entre VASP y sujetos obligados.

Settlement on-chain	Liquidación de operaciones o transferencias mediante redes blockchain o smart contracts, con trazabilidad, automatización y verificabilidad técnica.
Depósito tokenizado	Representación digital o tokenizada de una obligación o saldo emitido por una entidad autorizada, vinculada a dinero fiduciario o depósitos bajo régimen aplicable.
Market maker	Proveedor de liquidez que facilita formación de mercado, compra, venta o profundidad de libro bajo reglas de integridad, transparencia y prevención de manipulación.
Proveedor de liquidez	Persona o entidad que aporta liquidez a mercados digitales, pools, mesas OTC, plataformas o infraestructuras de settlement, sujeta a reglas proporcionales según riesgo y control efectivo.
EDD	Enhanced Due Diligence: debida diligencia reforzada aplicable a clientes, contrapartes, operaciones o jurisdicciones de mayor riesgo.
UBO	Ultimate Beneficial Owner o beneficiario final último: persona física que posee, controla o se beneficia efectivamente de una entidad, estructura o relación jurídica.
Source of Funds	Origen específico de los fondos utilizados en una transacción u operación determinada.
Source of Wealth	Origen patrimonial general de la riqueza de una persona o entidad.
Screening de sanciones	Proceso de verificación de personas, entidades, wallets, jurisdicciones o contrapartes contra listas de sanciones, terrorismo, proliferación u otros riesgos relevantes.
Stablecoin sistémica	Stablecoin cuyo volumen, alcance, uso en pagos, concentración, interconexión o función de liquidación puede generar impacto relevante sobre estabilidad financiera o integridad de mercado.
De-risking	Restricción o terminación indiscriminada de relaciones financieras por percepción general de riesgo, sin análisis individual, proporcionalidad o evaluación basada en conducta verificable.
Open Banking	Modelo de interoperabilidad financiera que permite compartir datos bancarios mediante APIs seguras, consentimiento del usuario y reglas de protección de datos.
Open Finance	Extensión del open banking a servicios financieros más amplios, incluyendo pagos, inversiones,

	seguros, activos digitales, crédito e infraestructura interoperable.
Cloud sovereignty	Soberanía cloud: capacidad de preservar control jurídico, técnico y operativo sobre datos, cargas de trabajo, llaves, jurisdicción, proveedores y continuidad en servicios de nube.
Multi-cloud	Arquitectura que utiliza múltiples proveedores o entornos cloud para reducir dependencia, mejorar resiliencia, portabilidad y continuidad operativa.
Infraestructura crítica digital	Sistemas, redes, datos, plataformas, llaves, registros, servicios o infraestructuras digitales cuya afectación podría comprometer seguridad nacional, servicios esenciales, democracia, estabilidad financiera o derechos fundamentales.
Criptografía post-cuántica	Técnicas criptográficas diseñadas para resistir amenazas derivadas de computación cuántica capaz de comprometer esquemas criptográficos tradicionales.
Neurocrímenes	Conductas ilícitas que afectan neurodatos, libertad cognitiva, privacidad mental, integridad mental, continuidad psicológica o dispositivos neurotecnológicos.
Captura tecnológica del Estado	Dependencia, control o influencia indebida sobre infraestructura pública digital por proveedores, plataformas, intereses privados, sistemas cerrados o actores extranjeros que comprometan soberanía, auditoría o continuidad institucional.
Arbitraje regulatorio abusivo	Uso de estructuras, jurisdicciones o tecnologías para eludir obligaciones esenciales de supervisión, protección al usuario, AML/CFT, transparencia o responsabilidad sin justificación económica legítima.
DLT	Distributed Ledger Technology o tecnología de registro distribuido. Incluye blockchain y otros sistemas digitales que permiten registrar, verificar o sincronizar información entre múltiples participantes o nodos.
Blockchain o tecnologías DLT	Expresión amplia utilizada para mantener neutralidad tecnológica cuando la norma comprende blockchain, registros distribuidos u otras arquitecturas equivalentes de verificación digital.
Inteligencia artificial	Sistema automatizado o modelo computacional capaz de generar resultados, recomendaciones, predicciones, clasificaciones, contenido o decisiones con base en datos, reglas, entrenamiento o inferencia algorítmica.

Tecnologías descentralizadas y emergentes	Categoría amplia que comprende blockchain, DLT, activos digitales, inteligencia artificial, computación avanzada, criptografía post-cuántica, neurotecnología, infraestructura digital, automatización y tecnologías futuras de impacto estratégico.
Web3	Ecosistema digital basado en redes descentralizadas, activos digitales, identidad soberana, smart contracts, tokenización, autocustodia y participación directa de usuarios.
Web3/Web4	Referencia narrativa a la evolución de ecosistemas descentralizados hacia arquitecturas integradas con inteligencia artificial, identidad soberana, computación avanzada, automatización y tecnologías emergentes.
CASP	Crypto-Asset Service Provider. Término utilizado en el marco MiCA de la Unión Europea. En esta ley se utiliza VASP como categoría principal, dejando CASP como referencia comparada.
Neurotecnología	Tecnología capaz de registrar, inferir, estimular, modificar o interactuar directa o indirectamente con actividad cerebral, procesos cognitivos, señales neuronales o estados mentales.
Delegación normativa técnica	Habilitación legal para que una autoridad competente emita lineamientos técnicos dentro de límites, finalidades, procedimientos y controles definidos por ley.
Proporcionalidad tecnológica	Principio conforme al cual toda medida tecnológica o regulatoria debe ser idónea, necesaria, razonable y menos invasiva frente al fin legítimo perseguido.
Reserva legal	Exigencia de que determinadas limitaciones a derechos fundamentales, sanciones, prohibiciones o competencias públicas estén establecidas por ley formal.
Legislación complementaria	Normativa futura que desarrolla aspectos específicos de una Ley Marco sin alterar sus principios estructurales ni sus garantías fundamentales.
Derecho comparado	Método de análisis que estudia marcos jurídicos extranjeros o internacionales para identificar referencias útiles, riesgos y adaptaciones aplicables al modelo costarricense.
Técnica legislativa	Conjunto de reglas de redacción, estructura, coherencia, precisión normativa y orden sistemático aplicables a la elaboración de leyes.

Homologación terminológica	Proceso de unificación del uso de conceptos técnicos y jurídicos para evitar contradicciones, duplicidades o interpretaciones divergentes dentro de un mismo cuerpo normativo.
Interoperabilidad regulatoria	Capacidad de coordinar estándares, licencias, supervisión, intercambio de información o reconocimiento entre autoridades, sin renunciar a soberanía regulatoria nacional.
Arbitraje regulatorio	Uso de diferencias normativas entre jurisdicciones para evadir obligaciones esenciales, reducir controles o desplazar riesgos hacia sistemas con menor supervisión.
Desconcentración máxima	Técnica de distribución de competencias dentro de una misma persona jurídica pública por la cual el órgano desconcentrado ejerce las materias atribuidas como propias, sin que el jerarca pueda avocar, revisar o sustituir sus decisiones ni impartir órdenes, instrucciones o circulares sobre esas materias, conforme al artículo 83 de la Ley General de la Administración Pública.
Derecho penal digital especial	Conjunto de tipos penales específicos destinados a proteger soberanía digital, infraestructura crítica, identidad digital, blockchain estatal, neurodatos, IA, smart contracts, stablecoins sistémicas y mercados digitales frente a conductas dolosas o gravemente lesivas.
Órgano técnico auxiliar especializado	Autoridad administrativa que, sin ejercer acción penal ni jurisdicción, colabora con el Ministerio Público, OIJ y autoridades competentes mediante informes técnicos, análisis forense, trazabilidad digital, inteligencia regulatoria y preservación de evidencia.
Unidad de Inteligencia y Análisis Tecnológico	Unidad especializada de la IID encargada de análisis blockchain, monitoreo de riesgos sistémicos, trazabilidad digital, análisis de smart contracts, stablecoins, IA, neurotecnología, infraestructura crítica y apoyo técnico a autoridades competentes.
Blockchain forensics	Conjunto de metodologías técnicas para analizar transacciones, wallets, contratos inteligentes, flujos de stablecoins, exposición ilícita, patrones de riesgo y evidencia on-chain.
Governance exploit	Explotación maliciosa de mecanismos de gobernanza digital, DAO, protocolo o smart contract para capturar decisiones, desviar activos, manipular parámetros o afectar derechos de usuarios.

Oracle attack	Manipulación, interferencia o corrupción de datos externos utilizados por un smart contract o infraestructura digital para generar resultados económicos, jurídicos o administrativos indebidos.
Bridge exploit	Explotación maliciosa de vulnerabilidades en puentes blockchain o mecanismos de interoperabilidad para sustraer, bloquear, duplicar o manipular activos digitales.
Rug pull sofisticado	Fraude digital mediante extracción maliciosa de liquidez, abandono planificado, manipulación de smart contracts, ocultamiento de control o simulación de descentralización con perjuicio a usuarios o inversionistas.
Cadena de custodia digital	Conjunto de procedimientos para preservar integridad, trazabilidad, autenticidad y admisibilidad de evidencia digital, on-chain, off-chain, criptográfica o algorítmica.
Mesa Nacional de Coordinación Penal Tecnológica	Mecanismo interinstitucional de coordinación entre Ministerio Público, OIJ, IID, UIF, MICITT, BCCR, SUGEF y otras autoridades para delitos de infraestructura digital, activos digitales y tecnologías emergentes.

PREÁMBULO / MANIFIESTO INTRODUCTORIO

Soberanía Digital de Costa Rica

Costa Rica nació como una República fundada sobre la dignidad humana, la libertad, la paz, la educación, la democracia y el respeto al Estado de Derecho. Su historia ha demostrado que una nación pequeña puede tomar decisiones civilizatorias grandes: una de las primeras capitales del mundo en contar con luz eléctrica en la historia, abolir el ejército, defender la institucionalidad democrática, proteger el ambiente y construir un modelo de convivencia basado en la legalidad, la libertad y la confianza pública.

Hoy, una nueva frontera histórica se abre ante nuestra generación, frente a nuestros propios ojos y algunos aún lo dimensionan.

La humanidad ha ingresado en una era en la que la identidad, el dinero, la propiedad, la información, la participación política y la vida social se trasladan aceleradamente hacia infraestructuras digitales. Lo que antes existía en documentos físicos, instituciones cerradas, registros territoriales y sistemas financieros tradicionales, ahora comienza a existir en redes, algoritmos, bases de datos, inteligencia artificial, activos digitales, contratos inteligentes y sistemas criptográficos.

Esta transformación no es meramente tecnológica. Es jurídica, económica, política y profundamente humana.

Porque quien controle la identidad digital, controlará el acceso a la vida pública.
Quien controle el dinero digital, controlará la libertad económica.
Quien controle los datos personales, controlará la intimidad.

Quien controle los registros públicos, controlará la propiedad.
Quien controle la infraestructura digital del Estado, controlará el futuro de la democracia.

Por ello, Costa Rica debe decidir desde ahora si la era digital será construida sobre vigilancia, centralización, dependencia e intermediación obligatoria, o si será construida sobre libertad, transparencia, descentralización, privacidad, innovación y soberanía individual.

Este Proyecto parte de una convicción esencial:

"La tecnología no debe convertirse en una herramienta para controlar al ser humano; debe convertirse en una infraestructura para proteger su libertad".

La digitalización del Estado no puede significar la creación de una arquitectura de vigilancia permanente sobre los ciudadanos. La modernización financiera no puede convertirse en una excusa para eliminar la autocustodia, prohibir la interacción directa entre personas o imponer intermediarios obligatorios sobre la economía digital. La identidad digital no puede ser una base de datos centralizada al servicio del poder, sino una extensión protegida de la personalidad jurídica, la dignidad humana y la autodeterminación informativa.

Costa Rica debe defender un principio fundamental para el siglo XXI:

"El Estado debe ser transparente ante el ciudadano; no solo el ciudadano transparente ante el Estado".

"La tecnología blockchain, los registros distribuidos, la criptografía, los activos digitales, la identidad autosoberana, los contratos inteligentes y las finanzas descentralizadas representan una oportunidad histórica para reconstruir la confianza pública, combatir la corrupción, reducir la opacidad administrativa y abrir una nueva etapa de libertad económica".

Blockchain no debe ser entendido únicamente como una innovación financiera, ni como una herramienta especulativa. Debe ser reconocido como una infraestructura pública de integridad, trazabilidad y verificación; una arquitectura capaz de convertir los actos del Estado en hechos auditables, los registros públicos en sistemas incorruptibles, la contratación pública en procesos verificables y la ejecución presupuestaria en información transparente para la ciudadanía.

La corrupción prospera donde los sistemas pueden alterarse sin dejar rastro.
La arbitrariedad prospera donde el poder no puede ser auditado.
La concentración prospera donde los ciudadanos no pueden verificar.
La libertad se debilita cuando toda participación económica depende de permisos, intermediarios o infraestructuras cerradas.

Por ello, este Proyecto propone una nueva visión constitucional, jurídica e institucional para Costa Rica y la región: una República Digital Libre, "donde la innovación no sea tolerada como excepción, sino protegida como expresión legítima de la libertad humana".

Costa Rica debe reconocer que la identidad digital forma parte de la identidad personal y, por tanto, merece protección constitucional. Toda persona debe tener derecho al control, portabilidad, seguridad y soberanía sobre su identidad digital, sus credenciales verificables, sus llaves criptográficas y sus representaciones electrónicas de existencia jurídica en la red.

Costa Rica debe reconocer también la libertad financiera digital como una garantía esencial de la economía contemporánea. Toda persona debe tener derecho a invertir, ahorrar, intercambiar, transferir, custodiar y participar en redes económicas digitales, sin discriminación tecnológica indebida y sin obligación general de intermediación bancaria o financiera.

La autocustodia debe ser protegida como una expresión moderna del derecho de propiedad, de la libertad contractual y de la autonomía individual. Ninguna persona debería estar obligada a entregar el control de sus activos

digitales a un tercero para poder participar en la economía digital, salvo limitaciones legales excepcionales, proporcionales, motivadas y compatibles con los derechos fundamentales.

Este Proyecto rechaza toda forma de arquitectura financiera digital que permita vigilancia masiva, censura económica, expiración programable del dinero, bloqueo arbitrario de transacciones, discriminación algorítmica o control político del acceso financiero. La innovación monetaria no debe conducir a una sociedad de permisos permanentes.

Por esa razón, Costa Rica debe prohibir expresamente cualquier modelo de moneda digital estatal minorista que pueda convertirse en instrumento de control social, vigilancia financiera o sustitución coercitiva del dinero libremente utilizado por las personas. La modernización financiera debe fortalecer la libertad, no condicionarla.

El país necesita una regulación especializada, técnicamente independiente y funcionalmente desconcentrada, ubicada dentro del ministerio rector de ciencia, innovación y tecnología pero protegida frente a interferencias jerárquicas en las decisiones regulatorias concretas. La economía Web3 y Web4 requiere un marco propio: uno que proteja a los usuarios, combata el fraude, prevenga abusos, cumpla estándares internacionales y, al mismo tiempo, defienda la autocustodia, el software libre, la innovación abierta, la interoperabilidad y la descentralización real.

Este Proyecto no propone ausencia de reglas. Propone mejores reglas.

Reglas que distingan entre intermediarios y código abierto.
Entre custodia y autocustodia.
Entre fraude e innovación.
Entre vigilancia y transparencia.
Entre regulación legítima y captura institucional.
Entre protección del usuario y control del ciudadano.

“Costa Rica tiene la oportunidad de construir el marco regulatorio más avanzado del mundo para activos digitales, blockchain, DeFi, identidad digital soberana, tokenización de la economía, registros públicos programables y gobernanza anticorrupción”.

No para copiar modelos extranjeros sin criterio.
No para importar regulaciones diseñadas para mercados financieros tradicionales.
No para subordinar la innovación nacional a estructuras que no comprenden la descentralización.

Sino para tomar lo mejor de cada experiencia global y construir una vía costarricense: democrática, constitucional, abierta, soberana, transparente y profundamente respetuosa de la libertad individual.

El mundo está entrando en una etapa donde la inteligencia artificial podrá analizarlo todo, los gobiernos podrán digitalizarlo todo, los bancos podrán condicionar el acceso a todo y las plataformas podrán intermediarlo todo. Frente a esa concentración creciente, la descentralización no es una moda tecnológica: es una defensa institucional de la libertad.

“Costa Rica debe ser la nación que demuestre que la tecnología puede servir a la democracia sin destruir la privacidad; que la transparencia puede aplicarse al poder sin convertir al ciudadano en objeto de vigilancia; que la innovación financiera puede florecer sin sacrificar derechos fundamentales; y que una economía digital abierta puede coexistir con legalidad, integridad y responsabilidad”.

Este Proyecto nace con una finalidad superior:

DECLARAR QUE LA LIBERTAD TAMBIÉN DEBE EXISTIR EN EL ENTORNO DIGITAL.

Y que la soberanía del siglo XXI no pertenece únicamente a los Estados, sino también a las personas: a su identidad, a sus datos, a sus activos, a sus llaves, a sus decisiones económicas y a su derecho de participar en el futuro sin pedir permiso a estructuras cerradas.

Costa Rica puede liderar una nueva generación de democracias digitales.

Una democracia donde el ciudadano sea soberano sobre su identidad.
Donde el Estado sea verificable por diseño.
Donde la economía digital no dependa de intermediación obligatoria.
Donde la privacidad sea protegida y no sospechada.
Donde blockchain sea herramienta anticorrupción.
Donde Bitcoin y los activos digitales descentralizados sean reconocidos dentro de un marco de libertad financiera.
Donde la innovación sea política pública de Estado.
Donde la tecnología no concentre el poder, sino que lo distribuya.

Este es el llamado.

A las instituciones.
A la Asamblea Legislativa.
A las universidades.
A los emprendedores.
A los juristas.
A los desarrolladores.
A la comunidad Web3 y Web4.
A los ciudadanos que entienden que la libertad no se pierde de golpe, sino por capas, por sistemas, por permisos, por silencios y por infraestructura.

Costa Rica debe actuar antes de que la arquitectura digital del futuro sea decidida sin sus ciudadanos.

Porque si la libertad no se protege en el código, en la ley y en la Constitución, será reemplazada por sistemas que no pedirán permiso para desaparecerla.

Por tanto, declaramos la necesidad histórica de construir una nueva arquitectura jurídica para Costa Rica: una arquitectura de descentralización, soberanía digital, libertad financiera, identidad autosoberana, transparencia pública, innovación abierta y protección constitucional de los derechos digitales.

Este Proyecto es el inicio de esa arquitectura.

Costa Rica no debe llegar tarde al futuro.
Debe diseñarlo.

ARTICULADO DEL PROYECTO DE LEY

CAPÍTULO I — DERECHOS Y GARANTÍAS DIGITALES

SECCIÓN I — DERECHOS Y GARANTÍAS DIGITALES

Artículo 1. Derecho a la Identidad Digital Soberana

Toda persona tiene derecho al reconocimiento, control, protección, portabilidad, interoperabilidad y soberanía sobre su identidad digital.

La identidad digital constituye una extensión de la personalidad jurídica, la dignidad humana, la autonomía individual y la autodeterminación informativa de la persona. Comprende, entre otros elementos, sus credenciales digitales, firmas electrónicas, llaves criptográficas, identificadores descentralizados, representaciones electrónicas, atributos verificables, datos personales y cualquier mecanismo tecnológico que permita acreditar su existencia, voluntad, capacidad, reputación, titularidad o participación en entornos digitales.

Ninguna autoridad pública, entidad privada, institución financiera, plataforma tecnológica o proveedor de servicios digitales podrá apropiarse, condicionar, limitar, suspender, transferir, explotar o centralizar la identidad digital de una persona sin base legal expresa, consentimiento informado o resolución debidamente motivada conforme al debido proceso.

El Estado promoverá sistemas de identidad digital soberana, interoperable, descentralizada, segura y respetuosa de la privacidad, evitando modelos de vigilancia, concentración indebida de datos, dependencia tecnológica, discriminación algorítmica o control social.

La identidad digital no podrá ser utilizada para restringir arbitrariamente el acceso de una persona a servicios públicos, educación, salud, justicia, propiedad, participación política, servicios financieros, economía digital o infraestructura tecnológica esencial.

Artículo 2. Derecho a la Autodeterminación Informativa Digital

Toda persona tiene derecho a decidir sobre la recopilación, uso, almacenamiento, transferencia, tratamiento, interoperabilidad y eliminación de sus datos personales en entornos digitales.

Este derecho comprende la facultad de conocer, acceder, rectificar, portar, limitar, oponerse y revocar el tratamiento de datos personales, así como exigir que todo procesamiento automatizado o algorítmico sea transparente, proporcional, verificable y sujeto a control humano cuando pueda afectar derechos fundamentales.

El Estado deberá garantizar que los sistemas digitales públicos y privados respeten los principios de minimización de datos, finalidad legítima, proporcionalidad, seguridad, consentimiento informado, privacidad por diseño, privacidad por defecto y responsabilidad demostrable.

Queda prohibida la creación de sistemas de perfilamiento masivo, scoring social, vigilancia predictiva o clasificación automatizada de personas que puedan afectar su dignidad, libertad, reputación, acceso económico, participación cívica o derechos fundamentales.

Artículo 3. Derecho a la Privacidad Digital

Toda persona tiene derecho a la privacidad en sus comunicaciones, datos, dispositivos, identidad, actividad digital, historial transaccional, relaciones electrónicas y patrones de comportamiento en entornos digitales.

La privacidad digital solo podrá ser limitada mediante ley formal, bajo criterios de necesidad, proporcionalidad, finalidad legítima, control judicial o autoridad competente, y con estricta sujeción al debido proceso.

El uso de tecnologías digitales por parte del Estado no podrá convertirse en mecanismo de vigilancia generalizada, monitoreo permanente, identificación indiscriminada o control automatizado de la ciudadanía.

La seguridad pública, la prevención del delito, la protección de menores, la integridad financiera o la modernización administrativa no podrán invocarse como justificación para implementar sistemas de vigilancia masiva, escaneo indiscriminado de comunicaciones privadas, debilitamiento del cifrado, puertas traseras tecnológicas o identificación obligatoria para toda interacción digital lícita.

Artículo 4. Derecho a la Privacidad Financiera Digital

Toda persona tiene derecho a la privacidad financiera en entornos digitales, incluyendo la protección de su historial económico, patrimonio, transacciones, wallets, activos digitales, patrones de consumo, inversión, ahorro, intercambio y participación en redes financieras descentralizadas.

La privacidad financiera no constituye presunción de ilicitud.

El Estado podrá requerir información financiera digital únicamente conforme a la ley, mediante procedimientos proporcionales, motivados y compatibles con el debido proceso, la protección de datos personales y los derechos fundamentales.

Queda prohibido implementar sistemas que permitan vigilancia financiera masiva, monitoreo indiscriminado de transacciones lícitas, censura económica automatizada, bloqueo arbitrario de fondos, discriminación financiera algorítmica o control político del acceso a medios de pago, activos digitales o infraestructura económica digital.

Artículo 5. Derecho a la Libertad Financiera Digital

Toda persona tiene derecho a participar libremente en la economía digital, incluyendo la facultad de adquirir, poseer, invertir, ahorrar, intercambiar, transmitir, recibir, donar, heredar, custodiar y utilizar activos digitales, tecnologías descentralizadas, redes blockchain, protocolos Web3/Web4 y sistemas criptográficos lícitos.

La libertad financiera digital comprende el derecho a acceder a mercados digitales, utilizar infraestructura descentralizada, celebrar contratos inteligentes, participar en mecanismos de tokenización, utilizar wallets, interactuar con protocolos descentralizados y ejercer derechos patrimoniales sobre bienes digitales.

Ninguna persona podrá ser discriminada, excluida o limitada en el ejercicio de actividades lícitas por el solo hecho de utilizar tecnologías blockchain, activos digitales, Bitcoin, stablecoins, tokens, smart contracts, wallets no custodiales o sistemas descentralizados.

Las limitaciones a este derecho deberán ser excepcionales, proporcionales, expresas, técnicamente justificadas y compatibles con el Estado de Derecho.

Artículo 6. Derecho a la Autocustodia

Toda persona tiene derecho a poseer, controlar, administrar y custodiar directamente sus activos digitales mediante llaves privadas, wallets no custodiales, hardware wallets, smart contracts, sistemas criptográficos y tecnologías descentralizadas.

La autocustodia constituye una manifestación del derecho de propiedad, de la libertad contractual, de la privacidad financiera y de la autonomía individual en la economía digital en mundo globalizado por medio del internet.

Ninguna ley, reglamento, autoridad pública, entidad financiera o proveedor tecnológico podrá imponer como regla general la obligación de custodiar activos digitales mediante terceros, intermediarios, bancos, exchanges, custodios autorizados o plataformas centralizadas.

El Estado deberá proteger el derecho de las personas a interactuar directamente con redes descentralizadas y protocolos lícitos, sin perjuicio de las obligaciones aplicables a intermediarios que ejerzan custodia, administración, control operativo o prestación profesional de servicios sobre activos de terceros.

Artículo 7. Derecho a la Propiedad Digital

Toda persona tiene derecho a la propiedad, posesión, control, disposición, transferencia, gravamen, herencia y defensa jurídica de sus activos digitales, bienes tokenizados, credenciales verificables, NFTs, tokens, derechos digitales, datos patrimoniales y representaciones criptográficas de valor.

Los activos digitales lícitamente adquiridos forman parte del patrimonio de la persona y deberán ser protegidos conforme a los principios constitucionales de propiedad privada, seguridad jurídica, debido proceso y tutela judicial efectiva.

La forma tecnológica de representación de un derecho no disminuirá su protección jurídica.

El Estado deberá reconocer la validez de los registros distribuidos, firmas criptográficas, hashes, timestamps, smart contracts y otros mecanismos técnicos como medios de prueba, trazabilidad y acreditación de titularidad, conforme a la ley.

Artículo 8. Derecho de Acceso a Infraestructura Descentralizada

Toda persona tiene derecho a acceder, utilizar, desarrollar, ejecutar, validar, auditar e interactuar con infraestructura descentralizada lícita, incluyendo redes blockchain, nodos, validadores, smart contracts, protocolos DeFi, sistemas de identidad soberana, almacenamiento descentralizado y herramientas criptográficas.

El acceso a infraestructura descentralizada no podrá ser restringido arbitrariamente por el Estado, intermediarios financieros, proveedores tecnológicos, plataformas digitales o actores dominantes del mercado.

El Estado promoverá estándares abiertos, interoperabilidad, neutralidad tecnológica, resiliencia, descentralización efectiva y reducción de dependencias monopólicas en la infraestructura digital nacional.

Artículo 9. Derecho a la Protección de la Criptografía

Toda persona tiene derecho a utilizar tecnologías criptográficas para proteger su identidad, comunicaciones, activos, datos, transacciones, credenciales, propiedad digital e interacción en entornos digitales.

Queda prohibida la imposición general de puertas traseras, debilitamiento obligatorio del cifrado, acceso secreto masivo, escaneo indiscriminado de comunicaciones privadas o vulnerabilidades deliberadas en sistemas de seguridad digital.

Las limitaciones excepcionales al uso de criptografía deberán estar previstas por ley, responder a finalidad legítima, ser necesarias, proporcionales, individualizadas y sujetas a control judicial o autoridad competente.

La criptografía será reconocida como infraestructura esencial para la privacidad, la seguridad jurídica, la libertad financiera, la identidad soberana y la protección de derechos fundamentales en la era digital.

Artículo 10. Derecho al Debido Proceso Algorítmico

Toda persona tiene derecho a no ser sometida a decisiones automatizadas, algorítmicas o basadas en inteligencia artificial que afecten derechos fundamentales, acceso económico, identidad digital, reputación, servicios públicos, servicios financieros, propiedad digital o participación cívica, sin transparencia, explicación, revisión humana y posibilidad real de impugnación.

El Estado y los sujetos regulados deberán garantizar trazabilidad, auditabilidad, explicabilidad proporcional, control humano significativo y mecanismos de reparación frente a decisiones automatizadas que produzcan efectos jurídicos o materiales relevantes.

Queda prohibida la utilización de sistemas algorítmicos opacos para excluir, censurar, restringir, perfilar o discriminar personas en la economía digital.

Artículo 11. Derecho a la No Discriminación Tecnológica

Ninguna persona podrá ser discriminada por utilizar tecnologías descentralizadas, wallets no custodiales, activos digitales, Bitcoin, protocolos blockchain, identidad autosoberana, software libre, criptografía o tecnologías descentralizadas y emergentes lícitas.

El Estado deberá prevenir prácticas de exclusión bancaria, financiera, comercial o institucional basadas únicamente en el uso legítimo de tecnologías descentralizadas.

La gestión de riesgos, cumplimiento normativo, prevención de lavado de dinero y protección del consumidor deberán aplicarse de forma proporcional, objetiva y basada en conducta verificable, no en prejuicio tecnológico.

Artículo 12. Derecho a la Portabilidad e Interoperabilidad Digital

Toda persona tiene derecho a la portabilidad de sus datos, identidad digital, credenciales verificables, historial reputacional, activos digitales, registros patrimoniales y relaciones digitales, conforme a estándares abiertos, seguros e interoperables.

Ninguna plataforma pública o privada podrá imponer mecanismos de bloqueo tecnológico, dependencia contractual abusiva o formatos cerrados que impidan el ejercicio efectivo de este derecho.

La interoperabilidad será principio esencial para evitar monopolios digitales, dependencia tecnológica y captura de la identidad o patrimonio digital de las personas.

Artículo 13. Derecho a la Educación y Alfabetización Digital Financiera

Toda persona tiene derecho a recibir educación digital, financiera y tecnológica que le permita comprender los riesgos, derechos, obligaciones y oportunidades de la economía digital, blockchain, activos digitales, ciberseguridad, autocustodia, privacidad y protección de datos.

El Estado promoverá programas de alfabetización digital y financiera orientados a prevenir fraude, manipulación, exclusión tecnológica y abuso contra consumidores, sin desalentar la innovación ni criminalizar el uso legítimo de tecnologías emergentes.

Artículo 14. Derecho a la Tutela Judicial Efectiva en Entornos Digitales

Toda persona tendrá derecho a tutela judicial efectiva para defender su identidad digital, activos digitales, datos, privacidad, credenciales, reputación, propiedad digital, autocustodia y participación en la economía digital.

El Poder Judicial deberá desarrollar capacidades técnicas para conocer controversias relacionadas con blockchain, activos digitales, contratos inteligentes, identidad digital, sistemas algorítmicos, prueba criptográfica y derechos digitales.

La ausencia de regulación específica no podrá utilizarse para negar protección judicial a derechos fundamentales ejercidos en entornos digitales.

Artículo 15. Cláusula de Interpretación Pro Libertad Digital

Las normas relativas a derechos digitales deberán interpretarse de conformidad con el principio pro persona, la dignidad humana, la libertad individual, la privacidad, la neutralidad tecnológica, la descentralización, la innovación responsable y la protección frente a vigilancia masiva.

En caso de duda interpretativa, deberá preferirse la interpretación que preserve la libertad digital, la privacidad, la autocustodia, la interoperabilidad, la descentralización efectiva y la soberanía individual, siempre dentro del marco del Estado de Derecho.

SECCIÓN II — NEURODERECHOS, LIBERTAD COGNITIVA Y PROTECCIÓN REFORZADA DE LA MENTE HUMANA

Artículo 16. Garantía Legal Reforzada de la Libertad Cognitiva

Toda persona tiene derecho a la libertad cognitiva, entendida como la facultad inviolable de preservar, decidir, desarrollar y autodeterminar su propio dominio mental, sus procesos de pensamiento, percepción, atención, memoria, emociones, razonamiento, voluntad y conciencia. Este derecho comprende decidir libremente si desea utilizar o rechazar neurotecnologías; no ser obligada directa o indirectamente a utilizar interfaces cerebro-computadora, dispositivos de estimulación cerebral, sistemas de monitoreo neuronal o tecnologías de medición cognitiva; conservar autonomía sobre sus procesos mentales internos; proteger su libertad de pensamiento frente a manipulación tecnológica, algorítmica, comercial, laboral, educativa, política o estatal; y recibir información clara, comprensible y previa sobre riesgos, beneficios, finalidades y alternativas antes de cualquier uso de neurotecnología. Ninguna autoridad pública, empresa, institución educativa, empleador, aseguradora, entidad financiera, plataforma tecnológica o proveedor de servicios digitales podrá condicionar derechos, empleo, educación, salud, crédito, seguros, participación política o acceso a servicios esenciales al uso obligatorio de neurotecnologías, salvo supuestos estrictamente médicos, terapéuticos, voluntarios, informados y regulados por ley.

Artículo 17. Protección Reforzada de la Privacidad Mental y de los Neurodatos

Toda persona tiene derecho a la privacidad mental, entendida como la protección reforzada de la actividad cerebral, datos neuronales, patrones cognitivos, estados emocionales, respuestas neurofisiológicas, inferencias mentales y cualquier información obtenida o inferida directa o indirectamente del sistema nervioso. Los neurodatos tendrán la categoría de datos sensibles de protección constitucional reforzada, incluso cuando sean procesados, anonimizados, inferidos, agregados o derivados por sistemas de inteligencia artificial, biometría, neurotecnología, sensores, wearables, dispositivos médicos, plataformas educativas, laborales, comerciales o de entretenimiento. Queda prohibido recolectar neurodatos sin consentimiento expreso, libre, informado, específico y revocable; vender, transferir o explotar neurodatos con fines comerciales abusivos; utilizar neurodatos para publicidad manipulativa, scoring, discriminación, perfilamiento político o vigilancia; inferir estados mentales sensibles sin base legal suficiente; tratar datos cerebrales como simples datos personales ordinarios; o exigir acceso a neurodatos como condición para empleo, educación, seguros, crédito, servicios públicos o participación política.

Artículo 18. Protección Reforzada de la Integridad Mental

Toda persona tiene derecho a la integridad mental, entendida como la protección contra intervenciones, manipulaciones, alteraciones, intrusiones o interferencias no consentidas, maliciosas, abusivas o desproporcionadas sobre su actividad cerebral, computación neuronal, emociones, percepción, memoria, conducta, voluntad o estado psicológico. Este derecho protege contra brain hacking, interferencias no autorizadas en interfaces cerebro-computadora, estimulación cerebral abusiva o no consentida, manipulación neurotecnológica de emociones, impulsos o decisiones, alteración de memoria, atención o percepción sin consentimiento válido, ataques cibernéticos contra dispositivos neuronales, uso de IA para inducir daño psicológico o dependencia cognitiva, y explotación de vulnerabilidades mentales mediante tecnología persuasiva abusiva. Toda neurotecnología médica, comercial, educativa, laboral o estatal deberá incorporar seguridad por diseño, ciberseguridad, auditoría, consentimiento informado, supervisión humana, protocolos de emergencia y responsabilidad por daño.

Artículo 19. Protección Reforzada de la Continuidad Psicológica e Identidad Personal

Toda persona tiene derecho a la continuidad psicológica, entendida como la preservación de su identidad personal, coherencia psicológica, autonomía decisional, memoria, preferencias, conducta, personalidad y sentido de sí misma

frente a influencias externas tecnológicas, algorítmicas, neurocomerciales o estatales. Este derecho protege frente a neuromarketing invasivo, manipulación emocional automatizada, estimulación cerebral dirigida a alterar preferencias o conducta, tecnologías persuasivas diseñadas para erosionar voluntad autónoma, IA o plataformas que exploten vulnerabilidades psicológicas, manipulación política, comercial, educativa o laboral basada en estados mentales inferidos, y modificación no consentida de patrones cognitivos o emocionales. Las tecnologías que puedan influir de forma significativa en comportamiento, personalidad, toma de decisiones o estabilidad emocional deberán someterse a controles reforzados de transparencia, consentimiento, evaluación de impacto, auditoría ética y prohibición de manipulación abusiva.

Artículo 20. Consentimiento Neurotecnológico Reforzado

Toda intervención neurotecnológica o tratamiento de neurodatos requerirá consentimiento previo, libre, informado, específico, verificable, revocable y separado de otros consentimientos generales. El consentimiento deberá incluir información clara sobre finalidad, tipo de datos recolectados, riesgos físicos, psicológicos, cognitivos y tecnológicos, uso de IA o análisis automatizado, terceros con acceso, transferencias internacionales, plazo de conservación, posibilidad de revocatoria, medidas de seguridad y consecuencias de no consentir. No será válido el consentimiento obtenido mediante coerción, dependencia laboral, presión educativa, necesidad económica, asimetría informativa, diseño oscuro, manipulación emocional o condicionamiento indebido de servicios esenciales.

Artículo 21. Prohibición de Discriminación Neurotecnológica

Se prohíbe toda discriminación basada en neurodatos, patrones cognitivos, inferencias mentales, condiciones neurobiológicas, uso o rechazo de neurotecnologías, capacidades cognitivas aumentadas, estados emocionales inferidos o perfiles psicológicos automatizados. Ninguna persona podrá ser excluida, sancionada, perfilada o tratada de manera desfavorable en empleo, educación, seguros, crédito, salud, justicia, servicios digitales, participación política o acceso a servicios públicos por razones derivadas de su información cerebral o mental, salvo justificación objetiva, proporcional y legalmente autorizada.

Artículo 22. Neurotecnología, Inteligencia Artificial y Garantías Legales de Supervisión

Toda neurotecnología integrada con inteligencia artificial, sistemas automatizados, plataformas digitales, biometría avanzada o dispositivos conectados deberá estar sujeta a regulación reforzada cuando pueda afectar libertad cognitiva, privacidad mental, integridad mental o continuidad psicológica. El Estado deberá exigir, según riesgo, evaluación de impacto neurotecnológico, auditoría algorítmica, ciberseguridad reforzada, transparencia funcional, supervisión humana, mecanismos de reparación, trazabilidad de decisiones automatizadas, prohibición de manipulación abusiva y control sobre transferencias internacionales de neurodatos.

Artículo 23. Protección Reforzada de la Mente Humana

La actividad mental, la conciencia, la voluntad, la identidad personal, los procesos cognitivos y los datos cerebrales constituyen una esfera de protección constitucional reforzada. Ninguna tecnología, política pública, contrato, plataforma, dispositivo, algoritmo, autoridad o empresa podrá invadir, manipular, capturar o explotar dicha esfera sin habilitación legal suficiente, consentimiento válido, finalidad legítima, proporcionalidad estricta y garantías efectivas.

SECCIÓN III — PROTECCIÓN INTEGRAL DE NIÑOS, NIÑAS Y ADOLESCENTES EN ENTORNOS DIGITALES

Artículo 24. Interés Superior de la Persona Menor de Edad en Entornos Digitales

Toda política pública, plataforma, sistema algorítmico, servicio digital, videojuego, red social, aplicación educativa, herramienta de inteligencia artificial, identidad digital, dispositivo conectado o infraestructura tecnológica que involucre niños, niñas o adolescentes deberá interpretarse conforme al interés superior de la persona menor de edad, su dignidad, desarrollo integral, privacidad, seguridad, autonomía progresiva y derecho a crecer en entornos digitales saludables. El diseño tecnológico dirigido a menores o utilizado materialmente por menores deberá adoptar estándares reforzados de protección por diseño, privacidad por defecto, minimización de datos, transparencia comprensible, accesibilidad, no discriminación y seguridad.

Artículo 25. Derecho al Desarrollo Cognitivo, Emocional y Digital Saludable

Los niños, niñas y adolescentes tienen derecho a un desarrollo cognitivo, emocional, social y digital saludable frente a tecnologías diseñadas para inducir dependencia, compulsión, hiperestimulación, comparación social dañina, manipulación emocional o exposición permanente a sistemas de recompensa algorítmica. El Estado promoverá estándares para prevenir diseños adictivos, patrones oscuros, manipulación dopaminérgica, notificaciones abusivas, recompensas variables orientadas a dependencia y mecanismos que exploten vulnerabilidades evolutivas de personas menores de edad.

Artículo 26. Prohibición de Manipulación Algorítmica Infantil

Queda prohibido utilizar algoritmos, sistemas de recomendación, inteligencia artificial, neurotecnología, diseño persuasivo o interfaces digitales para manipular de forma abusiva la conducta, emociones, preferencias, consumo, permanencia, interacción social, opinión política, percepción corporal o decisiones económicas de niños, niñas y adolescentes. Las plataformas deberán implementar controles reforzados contra microsegmentación abusiva, personalización opaca, explotación de vulnerabilidades psicológicas y recomendación automatizada de contenidos perjudiciales para el desarrollo integral.

Artículo 27. Protección Reforzada de Datos de Niños, Niñas y Adolescentes

Los datos personales, biométricos, conductuales, educativos, emocionales, geográficos, transaccionales, neuronales, de salud, interacción, rendimiento, atención, voz, imagen o inferencias psicológicas de niños, niñas y adolescentes serán datos de protección reforzada. Se prohíbe su explotación comercial abusiva, venta, perfilamiento permanente, reutilización incompatible, entrenamiento de modelos sin base legítima suficiente, vigilancia educativa desproporcionada o transferencia internacional sin garantías reforzadas. El tratamiento deberá limitarse a finalidad legítima, proporcionalidad, minimización, seguridad, consentimiento válido conforme a edad y madurez, intervención parental cuando corresponda y protección de autonomía progresiva.

Artículo 28. Límites a la Inteligencia Artificial Generativa frente a Menores

Los sistemas de inteligencia artificial generativa que interactúen con niños, niñas o adolescentes deberán cumplir reglas reforzadas de seguridad, transparencia, edad apropiada, prevención de manipulación, trazabilidad, supervisión humana, control parental razonable, protección de datos y mitigación de riesgos psicológicos, educativos, reputacionales y de suplantación. Queda prohibido diseñar IA generativa para inducir dependencia emocional, simular vínculos afectivos abusivos, explotar vulnerabilidades, fomentar aislamiento, manipular

decisiones, recopilar datos sensibles innecesarios o sustituir indebidamente acompañamiento humano esencial.

Artículo 29. Prohibición de Neuromarketing Infantil y Publicidad Neurodirigida

Queda prohibido utilizar neurodatos, biometría emocional, análisis de atención, seguimiento ocular, respuesta fisiológica, inferencias psicológicas o tecnologías equivalentes para dirigir publicidad, propaganda, consumo, apuestas, productos financieros, activos digitales, contenido político o conductas comerciales a niños, niñas y adolescentes. Las técnicas de persuasión comercial dirigidas a menores deberán ser transparentes, proporcionales, no abusivas y compatibles con su desarrollo evolutivo.

Artículo 30. Alfabetización Digital Crítica para Menores

El Estado deberá promover programas de alfabetización digital crítica para niños, niñas y adolescentes, incluyendo privacidad, ciberseguridad, identidad digital, inteligencia artificial, manipulación algorítmica, desinformación, activos digitales, autocustodia responsable conforme a edad, reputación digital, consentimiento, huella digital, bienestar tecnológico y derechos fundamentales en línea. Dichos programas deberán involucrar a familias, docentes, instituciones educativas, comunidades y autoridades competentes.

Artículo 31. Derecho a Espacios Digitales Seguros, Adecuados y No Explotativos

Los servicios digitales utilizados por menores deberán ofrecer entornos adecuados a la edad, mecanismos de denuncia, configuración de privacidad reforzada, límites frente a contacto abusivo, prevención de fraude, protección frente a explotación económica o sexual, seguridad frente a suplantación y medidas contra acoso, extorsión, grooming, manipulación y violencia digital. Estas obligaciones deberán aplicarse con respeto a libertad de expresión, acceso a información, autonomía progresiva y no vigilancia masiva.

Artículo 32. Evaluación de Impacto Digital en Servicios Dirigidos a Menores

Las plataformas, proveedores o sistemas digitales de alto impacto dirigidos a menores o utilizados significativamente por ellos deberán realizar evaluaciones de impacto sobre infancia digital, privacidad, salud mental, seguridad, manipulación algorítmica, sesgos, adicción tecnológica, datos sensibles y riesgos de IA. La autoridad competente podrá requerir mitigaciones, auditorías, ajustes de diseño, transparencia adicional o suspensión de prácticas abusivas cuando exista riesgo grave para derechos de menores.

SECCIÓN IV — LIMITACIONES AL PODER DIGITAL DEL ESTADO

Artículo 33. Prohibición de Vigilancia Masiva Digital

Queda prohibida toda forma de vigilancia digital masiva, indiscriminada, permanente o generalizada sobre la población.

Ninguna autoridad pública podrá implementar sistemas tecnológicos destinados a monitorear, rastrear, perfilar, clasificar, identificar o analizar de forma generalizada la vida digital, financiera, social, biométrica, comunicacional, transaccional o patrimonial de las personas.

La vigilancia digital solo podrá autorizarse de forma excepcional, individualizada, proporcional, temporal, motivada y conforme al debido proceso, mediante control judicial o autoridad competente expresamente habilitada por ley.

No podrán invocarse razones de seguridad pública, prevención del delito, integridad financiera, protección de menores, modernización estatal, eficiencia administrativa o innovación tecnológica para justificar la vigilancia generalizada de ciudadanos que no estén vinculados a una investigación concreta.

Artículo 34. Prohibición de Moneda Digital Estatal de Control Social

Queda prohibida la emisión, implementación o imposición obligatoria de una moneda digital estatal minorista que permita vigilancia financiera masiva, control programable del dinero, expiración de saldos, restricción arbitraria de transacciones, censura económica automatizada o condicionamiento político, ideológico, social o conductual del acceso financiero.

El Estado no podrá utilizar infraestructura monetaria digital para limitar, condicionar, bloquear, monitorear o programar el uso del dinero por parte de las personas, salvo medidas excepcionales autorizadas por ley, individualizadas, proporcionales, motivadas y sujetas a debido proceso.

La innovación monetaria pública no podrá sustituir coercitivamente el derecho de las personas a utilizar medios de pago lícitos, activos digitales descentralizados, efectivo, sistemas privados de pago, autocustodia o infraestructura financiera abierta.

Artículo 35. Prohibición de Scoring Social Estatal

Queda prohibida la creación, implementación o utilización de sistemas estatales de puntuación social, reputación obligatoria, clasificación ciudadana automatizada o perfiles conductuales destinados a condicionar derechos, libertades, servicios públicos, acceso financiero, movilidad, educación, empleo, participación política o acceso a infraestructura digital.

Ninguna autoridad podrá asignar puntajes, categorías, niveles de confianza, índices de comportamiento o clasificaciones algorítmicas generales a las personas con base en su actividad digital, financiera, social, política, religiosa, ideológica, comunicacional o económica.

La evaluación de riesgos en ámbitos específicos solo podrá permitirse cuando esté expresamente autorizada por ley, responda a una finalidad legítima, sea proporcional, limitada, verificable, no discriminatoria y sujeta a revisión humana efectiva.

Artículo 36. Prohibición de Censura Financiera Arbitraria

Queda prohibida toda forma de censura financiera arbitraria, bloqueo económico injustificado, exclusión digital, congelamiento automatizado, restricción bancaria o limitación de acceso a medios de pago, activos digitales, wallets, plataformas o infraestructura financiera lícita sin base legal expresa, motivación suficiente y debido proceso.

Ninguna persona podrá ser excluida del sistema financiero, bancario, digital o descentralizado por razones políticas, ideológicas, reputacionales, tecnológicas o por el solo hecho de utilizar activos digitales, Bitcoin, stablecoins, wallets no custodiales, protocolos descentralizados o infraestructura Web3/Web4 lícita.

Las medidas de congelamiento, bloqueo o limitación patrimonial deberán ser excepcionales, individualizadas, proporcionales, temporales y sujetas a control administrativo o judicial efectivo.

Artículo 37. Límites Legales al Uso Estatal de Inteligencia Artificial

El Estado podrá utilizar sistemas de inteligencia artificial únicamente cuando estos respeten la dignidad humana, los derechos fundamentales, la transparencia, la proporcionalidad, la seguridad, la no discriminación, la auditabilidad y el control humano significativo.

Queda prohibido el uso de inteligencia artificial estatal para vigilancia masiva, persecución política, censura automatizada, scoring social, manipulación ciudadana, identificación indiscriminada, represión de disidencia, discriminación algorítmica o control conductual de la población.

Todo sistema de inteligencia artificial utilizado por instituciones públicas que produzca efectos jurídicos, administrativos, financieros, patrimoniales o materiales sobre las personas deberá contar con:

a) Evaluación previa de impacto en derechos fundamentales.
b) Registro público del sistema utilizado.
c) Explicabilidad proporcional.
d) Mecanismo de revisión humana.
e) Auditoría técnica independiente.
f) Medidas de ciberseguridad y protección de datos.
g) Procedimientos de impugnación y reparación.

Artículo 38. Derecho al Pseudonimato Digital y al Anonimato Legítimo

Toda persona tiene derecho a utilizar pseudónimos, identificadores descentralizados, llaves criptográficas, wallets, credenciales selectivas y mecanismos de privacidad en entornos digitales lícitos.

El pseudonimato y el anonimato legítimo constituyen garantías de privacidad, libertad de expresión, libertad de asociación, seguridad personal, protección patrimonial y participación digital.

El Estado no podrá exigir identificación plena para toda interacción digital, transacción lícita, expresión en línea, participación en redes descentralizadas o uso de infraestructura tecnológica, salvo en los casos expresamente establecidos por ley y bajo criterios de necesidad, proporcionalidad y finalidad legítima.

Este derecho no ampara fraude, suplantación de identidad, lavado de dinero, financiamiento ilícito, abuso de menores, extorsión, terrorismo ni otras conductas tipificadas como delito.

Artículo 39. Prohibición de Interoperabilidad Coercitiva de Datos

Queda prohibida la integración obligatoria, indiscriminada o desproporcionada de bases de datos públicas y privadas que permita la construcción de perfiles integrales de la vida de las personas.

El Estado no podrá imponer sistemas de interoperabilidad que fusionen datos financieros, biométricos, fiscales, sanitarios, educativos, migratorios, electorales, judiciales, laborales, comerciales, de telecomunicaciones o identidad digital sin base legal expresa, finalidad específica, proporcionalidad estricta, garantías de minimización y mecanismos de control independiente.

La interoperabilidad digital deberá servir a la eficiencia pública y al ejercicio de derechos, no a la creación de expedientes totales de ciudadanos.

Artículo 40. Transparencia Algorítmica del Estado

Toda institución pública que utilice sistemas automatizados, algoritmos, inteligencia artificial, modelos predictivos, análisis de datos masivos o herramientas de decisión digital deberá garantizar transparencia, trazabilidad y rendición de cuentas.

Cuando dichos sistemas puedan afectar derechos, beneficios, obligaciones, sanciones, acceso financiero, identidad digital, propiedad, servicios públicos o participación ciudadana, la institución deberá publicar, como mínimo:

a) Finalidad del sistema.
b) Autoridad responsable.
c) Tipo de datos utilizados.
d) Criterios generales de funcionamiento.
e) Riesgos identificados.
f) Medidas de mitigación.
g) Procedimientos de revisión humana.
h) Mecanismos de impugnación.

No podrán invocarse secretos comerciales, seguridad nacional o confidencialidad tecnológica para ocultar sistemas que afecten derechos fundamentales, salvo reserva excepcional, motivada, proporcional y revisable por autoridad independiente.

Artículo 41. Prohibición de Arquitecturas Digitales Monopolísticas del Estado

El Estado no podrá diseñar, contratar o imponer infraestructura digital crítica que genere dependencia estructural de un único proveedor, una única plataforma, una única nube, una única blockchain, una única entidad financiera, una única identidad digital o un único sistema tecnológico cerrado.

Toda infraestructura digital pública crítica deberá diseñarse bajo principios de interoperabilidad, portabilidad, estándares abiertos, auditabilidad, resiliencia, continuidad operativa, soberanía tecnológica y prevención de captura corporativa.

Los contratos públicos de tecnología deberán incluir cláusulas de reversibilidad, acceso a documentación, auditoría técnica, portabilidad de datos, continuidad del servicio, transparencia de costos y prevención de dependencia tecnológica abusiva.

Artículo 42. Principio de Proporcionalidad Tecnológica

Toda medida estatal que utilice tecnologías digitales para limitar derechos fundamentales deberá cumplir los principios de legalidad, necesidad, idoneidad, proporcionalidad, temporalidad, mínima intervención, finalidad legítima, control independiente y revisión efectiva.

La autoridad deberá demostrar que la medida tecnológica adoptada:

a) Persigue una finalidad constitucionalmente legítima.
b) Es necesaria para alcanzar dicha finalidad.
c) Es la menos invasiva disponible.
d) No produce vigilancia generalizada.
e) No afecta de forma desproporcionada la privacidad, identidad, libertad financiera, autocustodia o libertad digital.
f) Cuenta con mecanismos de auditoría, impugnación y reparación.

Artículo 43. Prohibición de Puertas Traseras y Debilitamiento del Cifrado

Ninguna autoridad pública podrá exigir la inclusión de puertas traseras, vulnerabilidades deliberadas, mecanismos de acceso secreto, debilitamiento criptográfico o sistemas de escaneo indiscriminado en comunicaciones, wallets, dispositivos, protocolos, aplicaciones, redes descentralizadas o infraestructura digital privada.

Las investigaciones legítimas deberán realizarse mediante procedimientos individualizados, legalmente autorizados y compatibles con el debido proceso, sin comprometer la seguridad tecnológica general de la población.

Artículo 44. Prohibición de Identidad Digital Obligatoria Universal

El Estado no podrá imponer una identidad digital única, centralizada, obligatoria y universal como condición general para ejercer derechos, acceder a internet, participar en la economía digital, utilizar medios de pago lícitos, expresarse en línea, interactuar con redes descentralizadas o acceder a servicios privados.

Toda identidad digital pública deberá ser voluntaria, proporcional, interoperable, portable, segura, respetuosa de la privacidad y compatible con modelos de identidad autosoberana.

La identidad digital estatal no podrá convertirse en instrumento de exclusión, vigilancia, coerción o control social.

Artículo 45. Prohibición de Control Financiero Programable sobre Ciudadanos

Queda prohibida toda arquitectura estatal que permita programar, condicionar o restringir de forma generalizada el uso de fondos, activos, pagos, beneficios, tokens, monedas digitales o instrumentos financieros en una red, de una persona por razones no individualizadas o no sometidas a debido proceso.

El Estado no podrá crear mecanismos que permitan expirar dinero, limitar categorías de gasto, restringir geográficamente transacciones, condicionar fondos al comportamiento personal o bloquear automáticamente operaciones lícitas sin autorización legal específica y control efectivo.

Artículo 46. Prohibición de Fusión Opaca entre Estado, Bancos, Big Tech y Proveedores de Vigilancia

Queda prohibida la creación de sistemas digitales públicos que permitan la concentración opaca de datos, poder financiero, control tecnológico y capacidad de vigilancia entre instituciones estatales, entidades financieras, grandes plataformas tecnológicas, empresas de análisis de datos, proveedores de inteligencia artificial o contratistas de seguridad.

Todo convenio, contrato, alianza, integración técnica o sistema compartido entre el Estado y actores privados que involucre datos personales, financieros, biométricos, identidad digital, infraestructura crítica o sistemas algorítmicos deberá ser público, auditable y sujeto a control institucional independiente.

Artículo 47. Cláusula de Defensa frente al Autoritarismo y la Distopía Digital

Toda política pública, ley, reglamento, contrato, sistema tecnológico, plataforma estatal, arquitectura financiera digital, sistema de identidad, infraestructura de inteligencia artificial o mecanismo automatizado deberá interpretarse y ejecutarse conforme a la protección de la libertad humana en el entorno digital.

Se tendrá por contrario al orden constitucional todo sistema que, directa o indirectamente, tienda a:

a) Vigilar masivamente a la población.
b) Centralizar obligatoriamente la identidad digital.
c) Eliminar o restringir la autocustodia.
d) Imponer intermediación financiera obligatoria.
e) Censurar económicamente sin debido proceso.
f) Debilitar el cifrado.
g) Crear scoring social.
h) Fusionar bases de datos para control ciudadano.
i) Programar el dinero como instrumento de obediencia.
j) Sustituir libertad por permisos digitales permanentes.

SECCIÓN V — INFRAESTRUCTURA DIGITAL LIBRE Y DESCENTRALIZADA

Artículo 48. Derecho a la Infraestructura Descentralizada

Toda persona tiene derecho a acceder, utilizar, desarrollar, ejecutar, auditar, validar e interactuar con infraestructura digital descentralizada lícita.

Este derecho comprende redes blockchain, nodos, validadores, smart contracts, protocolos descentralizados, sistemas peer-to-peer, wallets no custodiales, identidad autosoberana, almacenamiento descentralizado, oráculos, sistemas criptográficos y demás tecnologías abiertas que permitan participación digital sin intermediación obligatoria.

El Estado no podrá restringir arbitrariamente el acceso a infraestructura descentralizada ni imponer barreras tecnológicas, regulatorias o financieras que hagan ilusorio su ejercicio.

Artículo 49. Protección del Código Abierto y del Software Libre

La creación, publicación, auditoría, mantenimiento, investigación, enseñanza, compilación, ejecución o distribución de código abierto, software libre, smart contracts, herramientas criptográficas, wallets no custodiales, nodos, validadores o protocolos descentralizados no constituirá por sí sola actividad financiera, intermediación, custodia, transmisión de dinero, captación pública, administración de activos de terceros ni prestación de servicios VASP.

La responsabilidad jurídica surgirá únicamente cuando exista custodia, control efectivo sobre activos de terceros, fraude, administración profesional de fondos, manipulación, ocultamiento deliberado de riesgos, captación ilícita o participación directa en actividades prohibidas por ley.

Artículo 50. Derecho a Operar Nodos y Validadores

Toda persona física o jurídica podrá operar nodos, validadores, infraestructura de consenso, infraestructura de indexación, oráculos, exploradores de blockchain y demás componentes técnicos de redes descentralizadas lícitas.

La operación de nodos o validadores no será considerada por sí sola intermediación financiera, custodia, emisión de activos digitales, prestación de servicios financieros ni actividad regulada, salvo que el operador ejerza control discrecional sobre activos de terceros o preste servicios sujetos a regulación especial.

El Estado promoverá la descentralización geográfica, institucional y técnica de nodos dentro del territorio nacional como medida de soberanía tecnológica, resiliencia digital y participación ciudadana.

Artículo 51. Protección Jurídica de Contratos Inteligentes (Smart Contracts)

Los “smart contracts” lícitamente desarrollados y ejecutados serán reconocidos como mecanismos tecnológicos válidos para automatizar obligaciones, transferencias, condiciones, registros, pagos, garantías, trazabilidad, certificaciones, verificaciones y ejecución de acuerdos digitales.

La validez jurídica de un acto no podrá rechazarse únicamente por haber sido ejecutado, registrado o verificado mediante smart contract, blockchain, firma criptográfica, hash, timestamp o sistema descentralizado.

La ley podrá establecer requisitos específicos cuando los smart contracts se utilicen para consumidores, servicios financieros, activos tokenizados, contratación pública, registros oficiales o actividades de alto impacto económico.

Artículo 52. Neutralidad Tecnológica y Protección de Derechos

El Estado deberá actuar bajo el principio de neutralidad tecnológica, evitando favorecer injustificadamente una red, protocolo, proveedor, lenguaje, plataforma, banco, nube, blockchain, arquitectura de identidad o infraestructura tecnológica específica.

La regulación deberá enfocarse en funciones, riesgos, control efectivo, custodia, impacto sistémico, protección de derechos y prevención de abusos, no en preferencias tecnológicas o presiones de actores dominantes.

Toda contratación pública, regulación técnica o política digital deberá justificar objetivamente cualquier preferencia tecnológica que limite interoperabilidad, competencia, descentralización o soberanía tecnológica.

Artículo 53. Interoperabilidad Abierta y Portabilidad

Toda infraestructura digital pública crítica deberá diseñarse bajo estándares abiertos, interoperables, auditables y portables.

Las personas tendrán derecho a trasladar sus datos, credenciales, identidad digital, activos digitales, registros, historial reputacional y relaciones digitales entre sistemas compatibles, sin dependencia abusiva de plataformas cerradas.

El Estado deberá promover APIs abiertas, documentación técnica, estándares verificables y mecanismos de interoperabilidad que permitan competencia, innovación, continuidad operativa y reducción de dependencia tecnológica.

Artículo 54. Prohibición de Dependencia Tecnológica Crítica

El Estado no podrá diseñar, contratar o implementar infraestructura digital crítica que genere dependencia irreversible, opaca o estructural respecto de un único proveedor, plataforma, nube, sistema operativo, blockchain, banco, identidad digital, modelo de inteligencia artificial o contratista tecnológico.

Toda infraestructura crítica deberá incluir cláusulas de reversibilidad, continuidad operativa, portabilidad de datos, documentación técnica, auditoría independiente, estándares abiertos, soberanía sobre información pública y capacidad de migración.

La dependencia tecnológica será considerada riesgo de soberanía nacional cuando afecte servicios esenciales, identidad digital, sistemas financieros, registros públicos, ciberseguridad, elecciones, salud, educación, justicia o seguridad pública.

Artículo 55. Soberanía Tecnológica Nacional

Costa Rica promoverá una política de soberanía tecnológica nacional orientada a fortalecer capacidades locales en blockchain, criptografía, ciberseguridad, inteligencia artificial, identidad digital soberana, infraestructura descentralizada, auditoría de código, tokenización y sistemas distribuidos.

El Estado fomentará alianzas con universidades, comunidades técnicas, sector privado, sociedad civil y organismos internacionales para desarrollar talento, investigación, infraestructura y estándares nacionales.

La soberanía tecnológica no implicará aislamiento, sino capacidad real de decidir, auditar, migrar, interoperar y no depender ciegamente de infraestructuras extranjeras cerradas.

Artículo 56. Protección contra Captura de Infraestructura Digital

Toda infraestructura digital pública o de relevancia sistémica deberá diseñarse con mecanismos anticaptura que impidan control indebido por parte de grupos económicos, plataformas tecnológicas, proveedores privados, instituciones financieras, operadores dominantes, contratistas estatales o intereses políticos.

Se considerarán mecanismos mínimos de prevención:

a) Gobernanza transparente.
b) Auditoría técnica independiente.
c) Publicación de estándares.
d) Registro de proveedores críticos.
e) Reglas de conflicto de interés.
f) Rotación y redundancia de proveedores cuando sea posible.
g) Evaluaciones periódicas de concentración tecnológica.
h) Control ciudadano cuando existan datos o recursos públicos involucrados.

Artículo 57. Resiliencia Digital Nacional

El Estado deberá garantizar que la infraestructura digital esencial sea resiliente, segura, auditable, distribuida, redundante y capaz de resistir fallas técnicas, ataques cibernéticos, dependencia externa, censura, desinformación, interrupciones de servicio y abuso de poder.

La resiliencia digital comprenderá, al menos:

a) Copias verificables y seguras de datos públicos críticos.
b) Infraestructura redundante.

c) Protocolos de recuperación ante incidentes.
d) Auditorías de ciberseguridad.
e) Capacidad nacional de respuesta técnica.
f) Mecanismos criptográficos de integridad.
g) Continuidad operativa de registros esenciales.
h) Protección de sistemas electorales, registrales, de salud, financieros y judiciales.

Artículo 58. Infraestructura Blockchain Pública de Integridad

El Estado podrá implementar infraestructura blockchain pública, híbrida o permisionada para garantizar integridad, trazabilidad, verificabilidad y auditabilidad de actos públicos, sin convertir dicha infraestructura en sistema de vigilancia ciudadana.

Esta infraestructura podrá utilizarse para contratación pública, Registro Público, catastro, presupuesto, licencias, concesiones, trazabilidad de fondos, deuda pública, activos tokenizados, certificaciones, documentos oficiales y auditoría institucional.

Los sistemas deberán diseñarse bajo minimización de datos, privacidad por diseño, uso de hashes, pruebas criptográficas, transparencia institucional y protección de datos personales.

Artículo 59. Derecho a Infraestructura Peer-to-Peer

Toda persona tendrá derecho a utilizar tecnologías peer-to-peer lícitas para intercambiar información, valor, credenciales, archivos, mensajes, activos digitales o servicios digitales sin intermediación obligatoria.

El uso de infraestructura peer-to-peer no podrá presumirse ilícito por su naturaleza descentralizada.

La regulación deberá distinguir entre el uso legítimo de redes descentralizadas y conductas ilícitas específicas cometidas mediante cualquier tecnología.

Artículo 60. Protección de Infraestructura de Privacidad

El Estado reconocerá la legitimidad de tecnologías de privacidad como cifrado, pruebas de conocimiento cero, firmas criptográficas, credenciales selectivas, wallets no custodiales, protocolos de minimización de datos, redes privadas y herramientas de seguridad digital.

Estas tecnologías no podrán ser prohibidas o restringidas por su capacidad de proteger privacidad, salvo en casos excepcionales, individualizados y conforme al debido proceso.

La privacidad técnica deberá considerarse componente esencial de ciberseguridad, libertad individual, seguridad patrimonial y protección frente a vigilancia indebida.

Artículo 61. Infraestructura Digital Pública como Bien de Interés Nacional

La infraestructura digital pública crítica será considerada bien estratégico de interés nacional cuando soporte derechos fundamentales, servicios esenciales, identidad digital, registros públicos, elecciones, sistemas financieros, salud, educación, justicia, seguridad o transparencia estatal.

Su diseño, operación, contratación y fiscalización deberán someterse a estándares reforzados de seguridad, transparencia, continuidad, independencia, protección de datos, neutralidad tecnológica y rendición de cuentas.

Artículo 62. Cláusula de Infraestructura Libre

Toda norma, contrato, política pública, reglamento, licitación o decisión administrativa relacionada con infraestructura digital deberá interpretarse de forma favorable a la apertura, interoperabilidad, auditabilidad, portabilidad, descentralización, seguridad, competencia, soberanía tecnológica y protección de derechos fundamentales.

Será contrario a este marco todo diseño que, sin justificación legítima y proporcional:

a) Imponga intermediación tecnológica obligatoria.
b) Bloquee interoperabilidad.
c) Encierre datos o identidades en sistemas cerrados.
d) Impida operar infraestructura descentralizada lícita.
e) Criminalice software neutral.
f) Debilite privacidad o cifrado.
g) Genere dependencia irreversible.
h) Concentre poder tecnológico sin controles.

CAPÍTULO II — BLOCKCHAIN COMO INFRAESTRUCTURA ANTICORRUPCIÓN Y DE TRANSPARENCIA PÚBLICA

SECCIÓN I — PRINCIPIOS DE TRANSPARENCIA PÚBLICA VERIFICABLE

Artículo 63. Principio de Transparencia Institucional Verificable

El Estado deberá promover el uso progresivo de tecnologías blockchain, registros distribuidos, criptografía, sellos de tiempo, hashes, firmas digitales, smart contracts y mecanismos de auditoría digital para garantizar la integridad, trazabilidad y verificabilidad de los actos públicos relevantes.

La transparencia institucional verificable comprende la posibilidad de que cualquier persona, órgano de control, autoridad judicial, medio de comunicación, universidad o entidad fiscalizadora pueda confirmar, mediante evidencia técnica, la existencia, secuencia, integridad y modificación de actos públicos, documentos, registros, procesos, contratos y decisiones administrativas.

La transparencia no deberá entenderse únicamente como acceso pasivo a documentos, sino como capacidad ciudadana de verificar que la información pública no ha sido alterada, ocultada o manipulada.

Artículo 64. Blockchain como Infraestructura Pública de Integridad

El Estado reconocerá blockchain y los registros distribuidos como infraestructura pública complementaria de integridad institucional, destinada a fortalecer la seguridad jurídica, la rendición de cuentas, la prevención de corrupción, la trazabilidad administrativa y el control ciudadano.

Su implementación deberá observar los principios de legalidad, neutralidad tecnológica, privacidad por diseño, minimización de datos, interoperabilidad, auditabilidad, seguridad, proporcionalidad y protección de derechos fundamentales.

La utilización de blockchain por parte del Estado no autorizará la creación de sistemas de vigilancia masiva, perfilamiento ciudadano, control financiero generalizado, identidad digital obligatoria centralizada o trazabilidad indiscriminada de la vida privada.

Artículo 65. Principio de Inmutabilidad, Trazabilidad y Memoria Institucional

Los actos públicos relevantes deberán contar con mecanismos técnicos que permitan conservar evidencia verificable de su origen, fecha, contenido, modificación, responsable, secuencia y estado.

La inmutabilidad no impedirá la corrección legal de errores, nulidades o rectificaciones; pero toda modificación deberá quedar registrada mediante historial verificable, preservando la trazabilidad completa del acto original y de sus cambios posteriores.

El Estado no podrá diseñar sistemas administrativos que permitan la eliminación retroactiva, edición invisible, sustitución no documentada o alteración opaca de información pública relevante.

SECCIÓN II — INTEGRIDAD REGISTRAL COMO POLÍTICA ANTICORRUPCIÓN Y REMISIÓN AL RÉGIMEN ESPECIAL

Artículo 66. Registro Público Blockchain como Eje de Integridad Institucional

El Registro Público, el Catastro y los registros administrativos estratégicos deberán incorporar progresivamente mecanismos blockchain, registros distribuidos, hashes, sellos de tiempo, certificaciones verificables y trazabilidad digital para fortalecer la integridad, publicidad, seguridad jurídica y auditabilidad de los actos registrales.

El desarrollo técnico, orgánico, notarial, registral y operativo de esta materia se regirá por el Capítulo XII de la presente ley, sin perjuicio de los principios anticorrupción establecidos en este capítulo.

Artículo 67. Smart Contracts Registrales como Herramienta de Integridad Pública

El Estado podrá utilizar smart contracts registrales para automatizar o verificar procesos previamente autorizados por ley, siempre que se preserven el debido proceso, la revisión humana, la seguridad jurídica y la protección de derechos de terceros.

Su regulación técnica y operativa se sujetará al Capítulo XII de esta ley.

Artículo 68. Evidencia Criptográfica de Actos Públicos

Los hashes, sellos de tiempo, firmas criptográficas, registros blockchain, trazas de smart contracts y certificaciones verificables podrán utilizarse como evidencia de integridad, existencia, secuencia y autenticidad de actos públicos conforme al régimen probatorio de esta ley.

El desarrollo procesal y probatorio especializado se regirá por el Capítulo XX.

Artículo 69. Catastro y Trazabilidad Territorial Anticorrupción

El Estado podrá utilizar infraestructura blockchain para fortalecer la trazabilidad territorial, prevenir alteraciones opacas, mejorar la interoperabilidad entre Registro Público, Catastro, municipalidades y autoridades competentes, y reducir riesgos de corrupción en información inmobiliaria o territorial.

El detalle técnico y operativo se desarrollará conforme al Capítulo XII.

SECCIÓN III — CONTRATACIÓN PÚBLICA PROGRAMABLE Y TRAZABILIDAD PRESUPUESTARIA

Artículo 70. Smart Contracts en Contratación Pública

El Estado podrá utilizar smart contracts en procesos de contratación pública para automatizar, registrar, verificar o ejecutar etapas previamente definidas de licitaciones, adjudicaciones, pagos, hitos, garantías, multas, cumplimiento contractual, entregables y órdenes de cambio.

La contratación pública programable deberá garantizar:

a) Publicidad del proceso.
b) Trazabilidad de ofertas.
c) Integridad de pliegos y modificaciones.
d) Registro verificable de adjudicaciones.
e) Historial de cambios contractuales.
f) Auditoría de pagos.
g) Control de hitos de ejecución.
h) Prevención de alteraciones retroactivas.
i) Revisión humana y recursos administrativos cuando correspondan.

El uso de smart contracts no podrá eliminar garantías de igualdad, competencia, debido proceso, impugnación, control interno ni fiscalización externa.

Artículo 71. Trazabilidad Presupuestaria On-Chain

El Estado deberá desarrollar mecanismos progresivos de trazabilidad presupuestaria mediante infraestructura blockchain o registros distribuidos para fondos públicos de alta relevancia, incluyendo infraestructura, programas sociales, compras públicas, transferencias, deuda pública, fondos especiales, fideicomisos públicos y proyectos estratégicos.

La trazabilidad presupuestaria deberá permitir verificar y fiscalizar en todo momento:

a) Origen de fondos.
b) Asignación presupuestaria.
c) Compromisos adquiridos.
d) Hitos de ejecución.
e) Pagos realizados.
f) Beneficiarios institucionales.
g) Modificaciones presupuestarias.
h) Saldos y ejecución acumulada.
i) Desviaciones, retrasos o incumplimientos.

La información publicada deberá proteger datos personales, secretos legítimos y seguridad institucional, sin impedir la auditoría ciudadana del uso de recursos públicos.

Artículo 72. Auditoría Ciudadana Blockchain

El Estado deberá garantizar herramientas públicas, accesibles y comprensibles para que la ciudadanía pueda auditar información pública anclada o registrada en blockchain.

La auditoría ciudadana podrá ejercerse mediante:

a) Exploradores públicos.
b) APIs abiertas.
c) paneles de trazabilidad.
d) Certificados verificables.
e) Repositorios de documentación.
f) Alertas de cambios relevantes.
g) Descarga de datos abiertos.
h) Integración con universidades, prensa, sociedad civil y órganos de control.

La participación ciudadana en la verificación de información pública no requerirá interés legítimo especial cuando se trate de datos públicos, fondos públicos, contratación estatal o actos administrativos de relevancia general.

Artículo 73. APIs Públicas, Datos Abiertos e Interoperabilidad Verificable

Toda infraestructura blockchain pública deberá diseñarse con APIs abiertas, estándares interoperables, documentación técnica, formatos de datos reutilizables y mecanismos de verificación accesibles.

El Estado deberá garantizar que la información pública relevante pueda ser consultada, auditada, reutilizada y analizada por órganos de control, academia, periodismo, sociedad civil, desarrolladores y ciudadanía.

Las APIs públicas no deberán permitir acceso indebido a datos personales o información sensible. Su diseño deberá equilibrar transparencia institucional, privacidad, seguridad y utilidad pública.

SECCIÓN IV — TOKENIZACIÓN PÚBLICA TRANSPARENTE

Artículo 74. Tokenización de Activos Públicos

El Estado podrá tokenizar activos públicos, derechos económicos, proyectos de infraestructura, concesiones, certificados, instrumentos financieros, bonos verdes, créditos ambientales, derechos de uso, participaciones en proyectos y otros activos autorizados por ley.

Toda tokenización pública deberá cumplir con:

a) Autorización legal o administrativa competente.
b) Inventario claro del activo subyacente.
c) Valoración técnica independiente cuando corresponda.
d) Registro público verificable.
e) Derechos y obligaciones del token claramente definidos.
f) Reglas de transferencia, custodia y ejecución.
g) Divulgación de riesgos.
h) Auditoría externa.
i) Trazabilidad de fondos.
j) Prohibición de opacidad patrimonial.

La tokenización no podrá utilizarse para evadir controles presupuestarios, endeudamiento público, contratación administrativa, responsabilidad fiscal, fiscalización legislativa o control de la Contraloría General de la República.

Artículo 75. Bonos Soberanos y Municipales Tokenizados

El Estado, sus instituciones y municipalidades podrán emitir instrumentos de deuda tokenizados, siempre que se cumplan íntegramente los requisitos constitucionales, legales, presupuestarios y de endeudamiento público aplicables al instrumento subyacente. La tokenización no modifica la naturaleza jurídica de la obligación ni reduce los controles exigibles por razón del emisor, la fuente de financiamiento o la jurisdicción de colocación.

Los bonos soberanos o municipales tokenizados deberán permitir, como mínimo: a) registro verificable de emisión; b) identificación del instrumento y condiciones financieras; c) trazabilidad de colocación; d) liquidación eficiente; e) registro de titulares conforme al marco aplicable; f) transparencia sobre uso de fondos; g) auditoría de pagos de intereses y amortización; y h) reportes públicos de ejecución del proyecto financiado.

La emisión de deuda tokenizada no podrá utilizarse para eludir controles fiscales, límites de endeudamiento, aprobación legislativa cuando corresponda, ni reglas de transparencia presupuestaria. Los empréstitos u operaciones financiadas con capital extranjero que se encuentren comprendidos en los supuestos constitucionales aplicables quedarán sujetos al procedimiento y mayoría que corresponda conforme a la Constitución Política.

Artículo 76. Prohibición de Tokenización Pública para Vigilancia o Control Social

Queda prohibido utilizar tokenización pública, bonos digitales, certificados estatales, beneficios sociales tokenizados, identidad digital, instrumentos financieros programables o infraestructura blockchain estatal para vigilancia masiva, control social, censura económica, expiración arbitraria de beneficios, discriminación algorítmica o condicionamiento político de derechos.

La programación de instrumentos públicos deberá respetar derechos fundamentales, debido proceso, proporcionalidad, finalidad legítima y revisión humana efectiva.

SECCIÓN V — GOBERNANZA, IMPLEMENTACIÓN Y CONTROL

Artículo 77. Implementación Progresiva y Prioridades Anticorrupción

La implementación de blockchain en el Estado deberá realizarse de forma progresiva, priorizando áreas de mayor impacto anticorrupción, riesgo de manipulación, volumen de fondos públicos, importancia registral o relevancia ciudadana.

Se considerarán áreas prioritarias:

a) Contratación pública.
b) Registro Público.
c) Catastro.
d) Presupuesto y gasto público.
e) Concesiones.
f) Licencias y permisos.
g) Fideicomisos públicos.
h) Deuda pública.
i) Programas sociales.
j) Infraestructura pública.
k) Compras de alto valor.
l) Fondos ambientales y climáticos.

Artículo 78. Evaluación de Impacto en Derechos Fundamentales

Todo sistema blockchain estatal deberá contar con una evaluación previa de impacto en derechos fundamentales, protección de datos, ciberseguridad, interoperabilidad, accesibilidad, sostenibilidad, riesgos de exclusión y posibilidad de vigilancia indebida.

La evaluación deberá publicarse, salvo reservas justificadas, y actualizarse periódicamente.

Ningún sistema podrá implementarse si su diseño genera vigilancia masiva, exposición indebida de datos personales, dependencia tecnológica crítica, discriminación algorítmica o afectación desproporcionada de derechos.

Artículo 79. Gobernanza Técnica y Auditoría Independiente

Los sistemas blockchain estatales deberán sujetarse a auditorías técnicas, jurídicas, financieras y de ciberseguridad, realizadas por órganos competentes o terceros independientes.

La auditoría deberá verificar:

a) Integridad del código.
b) Seguridad de smart contracts.
c) Gestión de llaves.
d) Resiliencia operativa.
e) Protección de datos.
f) Trazabilidad efectiva.
g) Cumplimiento normativo.
h) Riesgos de centralización.
i) Riesgos de captura tecnológica.
j) Mecanismos de reversión legal o corrección institucional.

Artículo 80. Gestión de Llaves Criptográficas Estatales

El Estado deberá establecer reglas estrictas para la creación, custodia, rotación, recuperación, autorización y uso de llaves criptográficas utilizadas en infraestructura pública blockchain.

La gestión de llaves deberá evitar concentración unipersonal, acceso no autorizado, pérdida irreversible, manipulación interna y dependencia de proveedores externos.

Se utilizarán mecanismos de multifirma, controles institucionales, separación de funciones, bitácoras verificables, auditoría periódica y protocolos de emergencia.

Artículo 81. Protección de Datos Personales en Blockchain Pública

Ninguna institución pública deberá registrar directamente en blockchain pública datos personales sensibles, biométricos, financieros, sanitarios, judiciales, familiares, electorales o de otra naturaleza protegida, salvo habilitación legal expresa, finalidad legítima y mecanismos técnicos adecuados.

La regla general será registrar pruebas de integridad, hashes, referencias, credenciales verificables, pruebas criptográficas o datos minimizados, evitando exposición irreversible de información personal.

Artículo 82. Cláusula Anticorrupción Digital

Será contrario al interés público todo diseño tecnológico, contrato, sistema, integración, proveedor o arquitectura estatal que permita:

a) Alterar registros sin trazabilidad.
b) Eliminar evidencia histórica.
c) Ocultar modificaciones contractuales.
d) Fragmentar información para impedir auditoría.
e) Centralizar llaves sin controles.
f) Crear dependencias opacas con proveedores.
g) Impedir acceso ciudadano a datos públicos.
h) Evadir fiscalización presupuestaria.
i) Programar fondos públicos sin reglas claras.
j) Sustituir transparencia por cajas negras tecnológicas.

CAPÍTULO III — SISTEMA FINANCIERO DESCENTRALIZADO Y LIBERTAD FINANCIERA DIGITAL

SECCIÓN I — PRINCIPIOS DE LIBERTAD FINANCIERA DIGITAL

Artículo 83. Reconocimiento de la Economía Digital Descentralizada

El Estado reconoce la existencia de una economía digital descentralizada basada en redes blockchain, activos digitales, Bitcoin, stablecoins, contratos inteligentes, protocolos DeFi, wallets no custodiales, tokenización, sistemas peer-to-peer e infraestructura criptográfica.

La economía digital descentralizada constituye una expresión legítima de la libertad económica, la innovación tecnológica, la propiedad privada, la libertad contractual, la autonomía individual y la participación en mercados globales.

El Estado deberá promover su desarrollo bajo principios de legalidad, protección al usuario, privacidad, autocustodia, neutralidad tecnológica, proporcionalidad regulatoria, prevención de fraude y respeto a la descentralización efectiva.

Artículo 84. Libre Participación Financiera Digital

Toda persona tiene derecho a participar libremente en la economía financiera digital, incluyendo adquirir, poseer, custodiar, invertir, intercambiar, transmitir, recibir, donar, heredar, utilizar y disponer de activos digitales lícitos.

Este derecho comprende la posibilidad de:

a) Usar wallets no custodiales.
b) Interactuar con protocolos descentralizados.
c) Participar en redes blockchain.
d) Utilizar Bitcoin y activos digitales descentralizados.
e) Utilizar stablecoins lícitas.
f) Celebrar contratos inteligentes.
g) Participar en tokenización de activos.
h) Realizar transacciones peer-to-peer lícitas.
i) Acceder a infraestructura financiera abierta.
j) Desarrollar servicios Web3/Web4 bajo reglas proporcionales.

Ninguna persona podrá ser excluida, discriminada o sancionada por participar lícitamente en esta economía.

Artículo 85. Bitcoin como Activo Financiero Descentralizado

Bitcoin será reconocido como activo digital descentralizado, sin emisor, sin administrador central, sin promesa de rendimiento por parte de terceros y sustentado en una red abierta, pública, global y verificable.

Bitcoin podrá ser utilizado lícitamente como:

a) Activo de reserva privada.
b) Medio de intercambio voluntario.
c) Instrumento contractual.
d) Colateral privado.
e) Bien patrimonial digital.
f) Activo de inversión.
g) Unidad de referencia económica cuando las partes así lo acuerden.
h) Activo transferible mediante autocustodia.

Bitcoin no será considerado por defecto valor mobiliario, deuda, depósito bancario, dinero electrónico emitido por tercero, promesa contractual de rendimiento ni instrumento sujeto a control de emisor.

Las operaciones con Bitcoin deberán analizarse conforme a su naturaleza descentralizada y al comportamiento específico de los sujetos participantes, no bajo categorías diseñadas para entidades emisoras centralizadas.

Artículo 86. Protección de la Autocustodia Financiera

Toda persona tiene derecho a custodiar directamente sus activos digitales mediante llaves privadas, wallets no custodiales, hardware wallets, multisignature wallets, smart contracts, protocolos descentralizados y demás mecanismos criptográficos lícitos.

La autocustodia no constituirá por sí misma actividad financiera regulada, custodia profesional, transmisión de dinero, intermediación, captación pública ni prestación de servicios VASP.

Ninguna autoridad podrá imponer como regla general que los activos digitales sean mantenidos exclusivamente en custodios, bancos, exchanges, entidades financieras o proveedores autorizados.

Las obligaciones regulatorias deberán recaer sobre quienes custodien, administren, controlen, intermedien o presten servicios profesionales sobre activos de terceros, no sobre la mera tenencia directa de activos propios.

SECCIÓN II — FINANZAS DESCENTRALIZADAS — DeFi

Artículo 87. Reconocimiento Jurídico de Protocolos DeFi

El Estado reconoce la existencia de protocolos de finanzas descentralizadas, entendidos como sistemas basados en contratos inteligentes (smart contracts), redes blockchain, mecanismos automatizados, liquidez programable y ejecución no custodial o parcialmente descentralizada de funciones financieras.

Los protocolos DeFi podrán facilitar, entre otros:

Intercambio descentralizado de activos.
b) Préstamos y créditos programables.
c) Provisión de liquidez.
d) Staking.
e) Colateralización.
f) Derivados descentralizados cuando sean autorizados.
g) Gestión automatizada de riesgos.
h) Pagos peer-to-peer.
i) Tokenización financiera.
j) Gobernanza descentralizada.

k) Tokenización de Activos del Mundo Real (RWA)

La existencia de un protocolo DeFi no implicará automáticamente la existencia de intermediario financiero, entidad regulada o prestador VASP. La calificación dependerá del grado de control efectivo, custodia, administración, centralización, gobernanza y participación económica identificable.

Artículo 88. Clasificación de Protocolos por Nivel de Descentralización

Los protocolos DeFi se clasificarán, para efectos regulatorios, según su nivel de descentralización efectiva:

a) Protocolos plenamente descentralizados:
Aquellos sin custodio, sin administrador central, sin control unilateral, sin capacidad discrecional de censura, sin modificación arbitraria de reglas y con gobernanza abierta o inmutable.

b) Protocolos con descentralización progresiva:
Aquellos que, durante una fase inicial, conservan ciertos mecanismos de actualización, gobernanza fundacional, control técnico limitado o administración temporal, con ruta pública hacia mayor descentralización.

c) Protocolos con control parcial:
Aquellos donde existen admin keys, control sobre front-end, control de oráculos, capacidad de actualizar contratos, modificar parámetros económicos, restringir usuarios o intervenir liquidez.

d) Protocolos administrados o centralizados con apariencia DeFi:
Aquellos donde una persona, empresa, grupo o entidad identificable ejerce control sustancial sobre operación, custodia, acceso, fondos, comisiones, gobernanza o condiciones esenciales del servicio.

Artículo 89. Regulación Proporcional Basada en Control Efectivo

La regulación aplicable a protocolos, interfaces, operadores o participantes DeFi deberá ser proporcional al grado de control efectivo que ejerzan sobre activos, usuarios, acceso, ejecución, parámetros, liquidez, información, gobernanza o riesgos del sistema.

Se considerarán indicadores de control efectivo:

a) Custodia de activos de terceros.
b) Capacidad de congelar, bloquear o revertir operaciones.

c) Control de admin keys.
d) Capacidad de actualizar smart contracts.
e) Control de front-end esencial.
f) Control de oráculos críticos.
g) Control de liquidez o liquidaciones.
h) Captura discrecional de comisiones.
i) Capacidad de censurar usuarios.
j) Promoción de rendimientos gestionados centralizadamente.
k) Administración de tesorería o gobernanza concentrada.
l) Control empresarial sobre la operación.

A mayor control efectivo, mayor obligación regulatoria. A menor control efectivo, mayor protección de la innovación descentralizada.

Artículo 90. Protección de Software No Custodial

El desarrollo, publicación, mantenimiento, auditoría, documentación, traducción, investigación, compilación, despliegue o distribución de software no custodial relacionado con DeFi no constituirá por sí solo actividad financiera regulada.

Tampoco constituirá por sí mismo prestación de servicios financieros:

a) Publicar código abierto.
b) Operar nodos.
c) Crear interfaces informativas.
d) Auditar smart contracts.
e) Proveer documentación técnica.
f) Desarrollar wallets no custodiales.
g) Participar en gobernanza descentralizada sin control efectivo.
h) Diseñar herramientas de privacidad lícita.
i) Desarrollar infraestructura peer-to-peer.

La responsabilidad surgirá cuando exista fraude, custodia, administración de activos de terceros, control operativo, captación, manipulación, ocultamiento de riesgos o participación directa en delitos.

Artículo 91. Derecho de Interacción Directa con Protocolos

Toda persona podrá interactuar directamente con protocolos descentralizados lícitos mediante wallets no custodiales, smart contracts, interfaces abiertas, nodos, APIs o infraestructura peer-to-peer.

El Estado no podrá imponer una obligación general de interacción exclusivamente mediante intermediarios autorizados, custodios, bancos, exchanges centralizados o plataformas supervisadas.

Podrán establecerse obligaciones específicas para intermediarios profesionales, interfaces comerciales, custodios, operadores con control efectivo o servicios ofrecidos masivamente al público, siempre bajo criterios de proporcionalidad, protección al usuario y respeto a la autocustodia.

SECCIÓN III — STABLECOINS, PAGOS DIGITALES Y TOKENIZACIÓN FINANCIERA

Artículo 92. Reconocimiento de Stablecoins

El Estado reconocerá las stablecoins como activos digitales diseñados para mantener referencia de valor respecto de una moneda, activo, cesta de activos u otro mecanismo económico verificable.

Las stablecoins podrán utilizarse lícitamente para pagos, liquidación, remesas, comercio digital, ahorro operativo, DeFi, tokenización, mercados digitales y otras finalidades permitidas por ley.

La regulación distinguirá entre:

a) Stablecoins respaldadas por reservas.
b) Stablecoins algorítmicas.
c) Stablecoins sobrecolateralizadas.
d) Stablecoins emitidas por entidades privadas.
e) Stablecoins descentralizadas.
f) Stablecoins utilizadas exclusivamente en protocolos.
g) Stablecoins de alcance sistémico.

Artículo 92 bis. Stablecoins e infraestructura de pagos fiat-digitales

La IID podrá formular recomendaciones, criterios técnicos y estándares interoperables sobre stablecoins, infraestructura de pagos fiat-digitales, interoperabilidad bancaria, liquidación digital, custodia institucional y sistemas de valor programable, en coordinación con el Banco Central de Costa Rica, SUGEF, CONASSIF, Ministerio de Hacienda y demás autoridades competentes.

La regulación específica de stablecoins sistémicas, emisores, reservas, auditorías, redención, custodia, liquidez, riesgo operacional, transparencia y supervisión prudencial será desarrollada mediante ley especializada y normativa técnica complementaria.

Ninguna disposición de esta ley autoriza emisión privada de moneda de curso legal, sustitución del colón costarricense, afectación de la política monetaria nacional o invasión de competencias del Banco Central de Costa Rica.

Artículo 93. Stablecoins no son Depósitos Bancarios por Defecto

La emisión, tenencia o uso de stablecoins no constituirá por sí sola depósito bancario, captación pública, dinero electrónico bancario, cuenta corriente, cuenta de ahorro ni obligación financiera asegurada por el Estado.

Una stablecoin solo será tratada como producto financiero equivalente a depósito cuando exista promesa de retorno fijo, captación de fondos con obligación de restitución, administración discrecional de reservas, garantía de rendimiento, publicidad como producto bancario o estructura económica equivalente.

Todo emisor o proveedor deberá informar claramente que una stablecoin no cuenta con garantía estatal ni seguro de depósitos, salvo autorización legal expresa.

Artículo 94. Transparencia, Reservas y Redención de Stablecoins

Las stablecoins ofrecidas al público desde Costa Rica o por entidades sujetas a la jurisdicción costarricense deberán cumplir reglas proporcionales de transparencia, pruebas de reservas, redención, auditoría, administración de riesgos y divulgación.

Según su naturaleza, podrán exigirse:

a) Identificación del emisor o responsable, cuando exista.
b) Composición de reservas.
c) Frecuencia de reportes.
d) Auditoría externa.
e) Políticas de redención.
f) Gestión de liquidez.
g) Riesgos de depeg.
h) Riesgos de contraparte.

i) Riesgos tecnológicos.
j) Reglas de gobernanza.
k) Divulgación clara al usuario.

Las stablecoins descentralizadas serán evaluadas conforme a su diseño, gobernanza, colateralización, grado de control y riesgo sistémico.

Artículo 95. Prohibición de Stablecoins Estatales de Vigilancia

Ninguna stablecoin, token público, instrumento de pago estatal, beneficio social tokenizado o activo digital emitido o promovido por el Estado podrá diseñarse para vigilancia masiva, control programable del gasto, expiración arbitraria, censura económica o condicionamiento conductual generalizado.

Los instrumentos digitales públicos deberán respetar privacidad, finalidad específica, proporcionalidad, debido proceso, seguridad, interoperabilidad y prohibición de control social.

SECCIÓN IV — INFRAESTRUCTURA FINANCIERA ABIERTA

Artículo 96. Derecho a Wallets No Custodiales

Toda persona tiene derecho a crear, descargar, portar, utilizar, desarrollar, auditar y controlar wallets no custodiales.

Las wallets no custodiales no serán consideradas por sí mismas entidades financieras, custodios, transmisores de dinero, emisores, exchanges, VASP ni intermediarios regulados, salvo que el proveedor asuma control efectivo sobre activos, llaves privadas, órdenes, fondos o ejecución económica de terceros.

El Estado no podrá prohibir wallets no custodiales ni exigir que toda wallet incorpore puertas traseras, identificación obligatoria universal, monitoreo masivo o control transaccional centralizado.

Artículo 97. Protección de Pagos Peer-to-Peer

Las personas podrán realizar pagos, transferencias, intercambios o liquidaciones peer-to-peer lícitas mediante activos digitales, Bitcoin, stablecoins, smart contracts, wallets no custodiales o redes descentralizadas.

La existencia de una transferencia peer-to-peer no implicará por sí sola actividad regulada, intermediación financiera o prestación profesional de servicios.

La ley podrá establecer obligaciones cuando exista actividad empresarial habitual, intermediación profesional, oferta pública de servicios, custodia de terceros, operación OTC organizada o riesgo sistémico.

Artículo 98. Interoperabilidad Financiera Abierta

El sistema financiero digital costarricense deberá promover interoperabilidad entre infraestructura tradicional y descentralizada, siempre que dicha interoperabilidad no elimine la autocustodia, no imponga intermediarios obligatorios y no genere vigilancia masiva.

La interoperabilidad deberá basarse en estándares abiertos, APIs, portabilidad, protección de datos, seguridad, privacidad, competencia y neutralidad tecnológica.

Los bancos, fintechs, VASP, protocolos, custodios, emisores de stablecoins y proveedores tecnológicos podrán integrarse bajo reglas técnicas proporcionales, sin monopolizar el acceso a la economía digital.

Artículo 99. Prohibición de Exclusión Bancaria Arbitraria

Ninguna entidad financiera, proveedor de pagos, banco, fintech, plataforma o institución regulada podrá excluir, cerrar cuentas, bloquear servicios, negar acceso o discriminar a una persona física o jurídica por la sola

circunstancia de participar lícitamente en actividades relacionadas con blockchain, Bitcoin, activos digitales, Web3, DeFi, tokenización o autocustodia.

Las decisiones de restricción o terminación de servicios deberán fundarse en un análisis individual, documentado y proporcional del riesgo, y podrán justificarse por obligaciones prudenciales, prevención de legitimación de capitales y financiamiento del terrorismo, fraude, sanciones internacionales aplicables, seguridad operativa, incumplimientos contractuales o regulatorios verificables u otras causas objetivas previstas por el ordenamiento.

Toda exclusión deberá ser motivada y comunicada en los términos permitidos por la legislación aplicable, y contar con mecanismos de revisión compatibles con el debido proceso y la gestión legítima de riesgos.

SECCIÓN V — REGULACIÓN ESPECIALIZADA Y REMISIÓN AL RÉGIMEN ORGÁNICO DE LA IID

Artículo 100. Autoridad Especializada en Activos Digitales y Blockchain

La regulación, supervisión, clasificación, promoción, autorización y ordenamiento del ecosistema de activos digitales, blockchain, DeFi, tokenización, VASP, mercados digitales e infraestructura financiera descentralizada corresponderá a la Intendencia de la Industria Descentralizada (IID), órgano técnico de desconcentración máxima adscrito al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, conforme al régimen orgánico establecido en el Capítulo XV de la presente ley.

Artículo 101. Separación Funcional frente al Sistema Financiero Tradicional

La regulación de la economía Web3 no quedará automáticamente subordinada a categorías diseñadas para banca, valores, seguros o intermediación financiera tradicional. La separación funcional, coordinación interinstitucional y límites regulatorios se regirán por el Capítulo XV.

Artículo 102. Competencias Especializadas por Remisión

Las competencias de clasificación, licenciamiento, supervisión, sandboxes, emisión de guías técnicas, protección de usuarios, cooperación internacional, transparencia on-chain y demás potestades de la IID serán las establecidas en el Capítulo XV.

Artículo 103. Financiamiento y Gestión Presupuestaria por Remisión

El régimen de financiamiento, programa presupuestario individualizado, tasas regulatorias, transparencia, auditoría y mecanismos anticaptura de la IID se regirá por el Capítulo XV y por las normas fiscales estratégicas del Capítulo XIV.

Los recursos destinados a la IID se incorporarán al Presupuesto Nacional y se administrarán conforme al ordenamiento financiero aplicable a los órganos desconcentrados del Gobierno Central, sin que dicha integración presupuestaria autorice interferencia en las competencias técnicas y regulatorias legalmente desconcentradas.

SECCIÓN VI — VASP Y SERVICIOS SOBRE ACTIVOS DIGITALES

Artículo 104. Proveedores de Servicios sobre Activos Digitales

Se considerarán proveedores de servicios sobre activos digitales las personas físicas o jurídicas que, de forma profesional, habitual y por cuenta de terceros, presten servicios de:

a) Custodia de activos digitales.
b) Intercambio entre activos digitales y moneda fiduciaria.
c) Intercambio entre activos digitales.
d) Transferencia de activos digitales por cuenta de terceros.
e) Administración de plataformas de negociación.

f) Colocación o distribución de activos digitales.
g) Servicios de brokerage o intermediación.
h) Administración de activos digitales de terceros.
i) Servicios OTC profesionales.
j) Emisión o gestión de stablecoins centralizadas.
k) Otros servicios definidos por la IID según riesgo y control efectivo.

No serán VASP por sí solos los usuarios, mineros, validadores, desarrolladores, operadores de nodos, proveedores de wallets no custodiales, auditores de código o participantes de redes descentralizadas sin custodia ni control de activos de terceros.

Artículo 105. Licenciamiento Proporcional de VASP

Los VASP estarán sujetos a registro, licenciamiento o autorización proporcional conforme a su actividad, volumen, riesgo, custodia, exposición al público, jurisdicción, gobernanza, controles internos y relevancia sistémica.

La IID podrá establecer categorías diferenciadas para:

a) Custodios.
b) Exchanges.
c) Brokers.
d) Plataformas de trading.
e) Emisores.
f) Proveedores de pagos.
g) Operadores DeFi con control efectivo.
h) Proyectos emergentes en sandbox.
i) Entidades institucionales.
j) Proveedores de infraestructura no custodial.

Artículo 106. AML/CFT Proporcional y Compatible con Autocustodia

Las obligaciones de prevención de lavado de dinero, financiamiento al terrorismo y financiamiento de proliferación deberán aplicarse de forma basada en riesgo, proporcional, tecnológicamente neutral y compatible con la autocustodia, privacidad financiera y derechos fundamentales.

La IID coordinará con las autoridades competentes para establecer obligaciones aplicables a intermediarios, custodios y VASP, sin convertir a usuarios no custodiales en entidades obligadas por el solo uso de tecnología descentralizada.

Las medidas AML/CFT no podrán justificar vigilancia masiva, prohibición general de wallets no custodiales, debilitamiento del cifrado, identificación obligatoria universal o criminalización de transacciones peer-to-peer lícitas.

Artículo 107. Travel Rule, Reporte Fiscal Internacional y Transferencias Digitales

La aplicación de la Travel Rule y de estándares equivalentes de prevención de legitimación de capitales y financiamiento del terrorismo se circunscribirá a los sujetos y transferencias comprendidos en la legislación especial aplicable, con enfoque basado en riesgo y respeto a la proporcionalidad.

Los marcos de reporte fiscal internacional, incluido el Crypto-Asset Reporting Framework (CARF) u otros que Costa Rica adopte conforme a su ordenamiento, se implementarán separadamente de las obligaciones AML/CFT y únicamente respecto de los sujetos, datos y operaciones comprendidos en la legislación tributaria y los instrumentos internacionales aplicables.

Las transferencias entre wallets no custodiales de usuarios no constituirán por sí mismas prestación de un servicio regulado. La IID coordinará con las autoridades competentes lineamientos técnicos que permitan cumplir

obligaciones internacionales sin eliminar la autocustodia, la privacidad financiera legítima ni la interacción peer-to-peer lícita.

SECCIÓN VII — PROTECCIÓN DEL USUARIO, MERCADO Y PUBLICIDAD

Artículo 108. Divulgación de Riesgos

Todo operador, emisor, intermediario, plataforma o proveedor regulado que ofrezca activos digitales al público deberá divulgar riesgos de forma clara, comprensible, visible, no engañosa y proporcional al producto o servicio.

La divulgación deberá incluir, cuando corresponda:

a) Riesgo tecnológico.
b) Riesgo de mercado.
c) Riesgo de liquidez.
d) Riesgo de contraparte.
e) Riesgo de custodia.
f) Riesgo de smart contract.
g) Riesgo de oráculos.
h) Riesgo de bridges.
i) Riesgo de pérdida de llaves.
j) Riesgo regulatorio.
k) Riesgo de stablecoin depeg.
l) Riesgo de gobernanza.

Artículo 109. Prohibición de Marketing Engañoso

Queda prohibida la publicidad engañosa, promesas de rendimiento garantizado, ocultamiento de riesgos, uso indebido de símbolos estatales, afirmaciones falsas de respaldo oficial, simulación de seguridad bancaria, manipulación de testimonios, presión comercial abusiva o promoción de activos digitales como libres de riesgo.

Toda comunicación comercial deberá distinguir claramente entre inversión, utilidad, pago, gobernanza, especulación, custodia, rendimiento y riesgos asociados.

Artículo 110. Protección frente a Fraude y Abuso de Mercado

La IID deberá establecer reglas para prevenir fraude, manipulación, insider trading, wash trading, rug pulls, falsificación de reservas, manipulación de oráculos, ataques coordinados, información falsa, abuso de usuarios y conductas equivalentes en mercados de activos digitales.

Estas reglas deberán aplicarse sin criminalizar volatilidad, fallas no dolosas, descentralización legítima o experimentación tecnológica transparente.

SECCIÓN VIII — CLÁUSULAS DE DEFENSA DE LA LIBERTAD FINANCIERA DIGITAL

Artículo 111. Prohibición de Intermediación Financiera Digital Obligatoria

Ninguna persona estará obligada a utilizar intermediarios financieros, bancarios, custodios, exchanges, proveedores autorizados, plataformas centralizadas o entidades reguladas para participar en la economía digital, salvo casos específicos establecidos por ley, justificados por riesgo concreto y compatibles con derechos fundamentales.

El Estado no podrá convertir la intermediación obligatoria en condición general de acceso a activos digitales, wallets, DeFi, Bitcoin, stablecoins, tokenización o pagos digitales lícitos.

Artículo 112. Prohibición de Captura Bancaria de la Economía Digital

Las autoridades públicas deberán evitar que el sistema financiero tradicional capture, bloquee o limite indebidamente el desarrollo de la economía digital descentralizada mediante exclusión bancaria, sobrerregulación, acceso discriminatorio, exigencias incompatibles, monopolio de licencias o barreras artificiales de entrada.

La coexistencia entre banca tradicional y Web3 deberá basarse en competencia, interoperabilidad, proporcionalidad y libertad de elección del usuario.

Artículo 113. Cláusula Pro Libertad Financiera Digital

Toda norma, reglamento, política pública o acto administrativo relacionado con activos digitales, Bitcoin, DeFi, stablecoins, VASP, tokenización, wallets, autocustodia, incluyendo identidades digitales o infraestructura financiera descentralizada, deberá interpretarse conforme al principio pro libertad financiera digital.

En caso de duda, deberá preferirse la interpretación que preserve:

a) Autocustodia.
b) Privacidad financiera.
c) Descentralización efectiva.
d) Interoperabilidad abierta.
e) Innovación responsable.
f) Derecho de propiedad digital.
g) Protección del usuario.
h) Prevención de fraude.
i) Cumplimiento proporcional.
j) Rechazo a vigilancia masiva.

CAPÍTULO IV — CLASIFICACIÓN FUNCIONAL DE LOS ACTIVOS DIGITALES

SECCIÓN I — PRINCIPIOS GENERALES DE CLASIFICACIÓN

Artículo 114. Principio de Clasificación Funcional

Los activos digitales serán clasificados conforme a su función económica, naturaleza técnica, derechos incorporados, grado de descentralización, existencia o inexistencia de emisor, nivel de control efectivo, uso previsto, riesgo para usuarios y posible impacto sistémico.

Ningún activo digital será clasificado únicamente por el hecho de utilizar blockchain, registros distribuidos, smart contracts, criptografía, tokenización o infraestructura descentralizada.

Artículo 115. Principio de No Recalificación Automática

Ningún activo digital será considerado automáticamente valor mobiliario, título valor, depósito bancario, dinero electrónico, instrumento financiero, derivado, commodity, medio de pago obligatorio, activo regulado o producto de inversión por el solo hecho de estar representado en blockchain o ser transferible digitalmente.

La calificación jurídica deberá realizarse caso por caso, conforme a los derechos, obligaciones, expectativas económicas, estructura de emisión, forma de comercialización, grado de descentralización y conducta de los sujetos intervinientes.

Artículo 116. Principio de Regulación Proporcional al Riesgo

La intensidad regulatoria aplicable a cada categoría de activo digital deberá ser proporcional a:

a) Existencia de custodia de terceros.
b) Existencia de emisor o promotor identificable.
c) Promesa de rendimiento.
d) Captación de fondos del público.
e) Riesgo de pérdida para usuarios.
f) Grado de liquidez.
g) Complejidad técnica.
h) Posible impacto sistémico.
i) Riesgo de fraude o manipulación.
j) Grado de descentralización.
k) Uso como medio de pago.
l) Existencia de reservas o colateral.
m) Nivel de información disponible para el público.

Artículo 117. Principio de Protección de la Autocustodia

La clasificación de activos digitales no podrá utilizarse para prohibir, restringir o desnaturalizar la autocustodia.

La mera tenencia, posesión, transferencia, recepción, uso, inversión, ahorro o resguardo de activos digitales propios mediante wallets no custodiales no constituirá por sí misma actividad financiera regulada, intermediación, custodia profesional, captación pública, emisión de activos, VASP ni prestación de servicios financieros.

Artículo 118. Principio de Compatibilidad con GAFI/FATF sin Vigilancia Masiva

Costa Rica aplicará los estándares internacionales de prevención de lavado de dinero, financiamiento del terrorismo y financiamiento de proliferación conforme a un enfoque basado en riesgo, de acuerdo con la Recomendación 15 de GAFI/FATF y demás estándares aplicables.

Las obligaciones AML/CFT deberán recaer sobre VASP, custodios, intermediarios, emisores, plataformas u operadores con control efectivo sobre activos o servicios de terceros.

La mera autocustodia, operación de nodos, desarrollo de software, interacción peer-to-peer, uso de wallets no custodiales o participación directa en protocolos descentralizados no convertirá a una persona en sujeto obligado por sí sola.

SECCIÓN II — CATEGORÍAS FUNCIONALES DE ACTIVOS DIGITALES

Artículo 119. Activos Digitales Descentralizados sin Emisor

Son activos digitales descentralizados sin emisor aquellos que existen en redes abiertas, públicas, distribuidas o descentralizadas, sin entidad emisora, administrador central, promotor responsable, obligación de redención, promesa de rendimiento o control unilateral por parte de terceros.

Se incluyen dentro de esta categoría Bitcoin y aquellos activos que cumplan condiciones equivalentes de descentralización efectiva.

Estos activos podrán utilizarse lícitamente como:

a) Bienes patrimoniales digitales.
b) Activos de reserva privada.
c) Medios de intercambio voluntario.
d) Activos de inversión.
e) Colateral contractual.
f) Instrumentos de transferencia de valor.

g) Activos autocustodiables.
h) Referencias económicas privadas cuando las partes así lo acuerden.

No serán considerados valores mobiliarios, depósitos bancarios, dinero electrónico, deuda, promesa contractual de rendimiento ni instrumentos emitidos por terceros por defecto.

Artículo 120. Bitcoin

Bitcoin será reconocido expresamente como activo digital descentralizado sin emisor, basado en una red pública, abierta, global, verificable y resistente a censura.

Bitcoin podrá ser adquirido, poseído, transferido, recibido, heredado, donado, utilizado como colateral, autocustodiado y empleado en contratos privados de forma lícita.

El Estado no podrá imponer intermediación obligatoria para la tenencia, transmisión o autocustodia de Bitcoin entre particulares, sin perjuicio de las obligaciones aplicables a intermediarios profesionales, custodios o VASP.

Las operaciones con Bitcoin adquiridas, mantenidas o transmitidas mediante autocustodia o redes descentralizadas deberán analizarse conforme a principios de libertad financiera, territorialidad fiscal, buena fe, trazabilidad razonable, prevención de abuso y respeto al derecho de propiedad digital.

Artículo 121. Tokens de Pago

Son tokens de pago aquellos activos digitales destinados principalmente a ser utilizados como medio de intercambio, transferencia de valor, liquidación, pago, remesa o unidad transaccional dentro de redes, plataformas o ecosistemas digitales.

Los tokens de pago no serán considerados moneda de curso legal, depósito bancario o dinero electrónico estatal por el solo hecho de cumplir función transaccional.

Cuando sean emitidos o administrados por entidad identificable, podrán estar sujetos a reglas de transparencia, protección al usuario, AML/CFT, reservas, redención, gobernanza o supervisión proporcional, según su diseño y riesgo.

Artículo 122. Stablecoins/ Monedas Estables

Son stablecoins aquellos activos digitales diseñados para mantener una referencia de valor respecto de una moneda uno a uno, activo, cesta de activos, mecanismo algorítmico, colateral o estructura económica determinada.

Las stablecoins se clasifican en:

a) Stablecoins respaldadas por reservas fiduciarias.
b) Stablecoins respaldadas por activos financieros.
c) Stablecoins sobrecolateralizadas.
d) Stablecoins algorítmicas.
e) Stablecoins descentralizadas.
f) Stablecoins emitidas por entidades privadas.
g) Stablecoins de uso cerrado o ecosistémico.
h) Stablecoins de relevancia sistémica.
i) Stablecoins vinculadas a activos reales.
j) Stablecoins híbridas.

Las stablecoins no serán consideradas depósitos bancarios por defecto, salvo que su estructura implique captación reembolsable, promesa de restitución equivalente, rendimiento fijo, garantía bancaria, administración discrecional de fondos o publicidad como producto equivalente a depósito.

Artículo 123. Tokens de Utilidad

Son tokens de utilidad aquellos activos digitales que otorgan acceso, uso, consumo, participación funcional o derechos operativos dentro de una red, aplicación, protocolo, plataforma, servicio digital o ecosistema tecnológico.

Los tokens de utilidad no serán considerados valores mobiliarios por defecto, salvo que sean ofrecidos principalmente como inversión, con expectativa razonable de ganancia derivada de esfuerzos empresariales o gerenciales de terceros, o que incorporen derechos económicos propios de instrumentos financieros.

La IID podrá establecer reglas de divulgación cuando los tokens de utilidad sean ofrecidos públicamente, con el fin de evitar publicidad engañosa, simulación de utilidad o venta de instrumentos de inversión disfrazados.

Artículo 124. Tokens de Gobernanza

Son tokens de gobernanza aquellos que confieren derechos de participación, votación, propuesta, decisión o coordinación dentro de protocolos, DAOs, redes descentralizadas o ecosistemas digitales.

Los tokens de gobernanza no serán considerados valores mobiliarios por el solo hecho de permitir votar o participar en decisiones técnicas.

Podrán requerir supervisión o reglas especiales cuando:

a) Otorguen derechos sobre ingresos, dividendos o flujos económicos.
b) Permitan control concentrado de tesorería.
c) Sean vendidos como inversión.
d) Confieran poder efectivo sobre activos de terceros.
e) Permitan modificar reglas financieras críticas.
f) Exista concentración sustancial en promotores o insiders.
g) Se utilicen para manipular mercados o capturar gobernanza.

Artículo 125. Tokens de Inversión o Security Tokens

Son tokens de inversión o security tokens aquellos activos digitales que representen, incorporen o confieran derechos económicos equivalentes a acciones, deuda, participaciones, dividendos, intereses, rendimientos, beneficios, flujos financieros, derechos sobre utilidades, instrumentos colectivos de inversión o expectativas de ganancia derivadas principalmente de esfuerzos de terceros.

Estos tokens estarán sujetos a un régimen especial de divulgación, autorización, registro o supervisión proporcional, bajo competencia primaria de la IID y coordinación con autoridades competentes cuando corresponda.

La tokenización de un instrumento financiero tradicional no eliminará los derechos del inversionista ni los deberes del emisor; únicamente modificará la forma tecnológica de representación, transferencia, liquidación y trazabilidad.

Artículo 126. Tokens Representativos de Activos Reales — RWA

Son tokens representativos de activos reales aquellos que representan, referencian o incorporan derechos sobre bienes físicos, bienes inmuebles, infraestructura, commodities, energía, carbono, facturas, créditos, propiedad intelectual, maquinaria, inventarios, concesiones, derechos contractuales, flujos económicos o cualquier otro activo del mundo real.

Su régimen deberá garantizar:

a) Existencia y titularidad del activo subyacente.
b) Determinación clara de derechos del titular del token.
c) Custodia o administración del activo subyacente, cuando aplique.
d) Reglas de transferencia.
e) Divulgación de riesgos.

f) Mecanismos de ejecución.
g) Auditoría o certificación independiente cuando corresponda.
h) Relación jurídica entre token y activo subyacente.
i) Protección frente a doble emisión o doble gravamen.
j) Interoperabilidad con registros públicos cuando aplique.

Artículo 127. Tokens No Fungibles — NFT

Son tokens no fungibles aquellos activos digitales únicos o identificables individualmente, que pueden representar arte, coleccionables, identidad, membresías, certificaciones, derechos de acceso, propiedad intelectual, objetos digitales, activos del mundo real o derechos específicos.

Los NFT se clasifican en:

a) NFT artísticos o coleccionables.
b) NFT de membresía o acceso.
c) NFT de identidad o credencial.
d) NFT de propiedad intelectual.
e) NFT representativos de activos reales.
f) NFT financieros o fraccionados.
g) NFT con derechos económicos.
h) NFT de certificación pública o privada.

Un NFT no será considerado instrumento financiero por el solo hecho de ser transferible o tener valor de mercado. Será regulado conforme a los derechos que incorpore, la forma de comercialización, la expectativa económica ofrecida y el grado de control de terceros.

Artículo 128. Credenciales Verificables, Tokens de Identidad y Reputación

Son credenciales verificables, tokens de identidad o tokens reputacionales aquellos que acreditan atributos, calificaciones, permisos, títulos, certificaciones, licencias, identidad, membresías, historial reputacional, cumplimiento, experiencia, participación o estados verificables de una persona, entidad o sistema.

Estos tokens no serán considerados activos financieros por defecto y estarán sujetos prioritariamente a reglas de identidad digital soberana, protección de datos, privacidad, interoperabilidad, portabilidad y no discriminación.

Queda prohibida su utilización para scoring social, vigilancia masiva, exclusión económica automatizada o perfilamiento indebido.

Artículo 129. Tokens Públicos o Estatales

Son tokens públicos o estatales aquellos emitidos, reconocidos o utilizados por el Estado, instituciones públicas, municipalidades o entes públicos para representar certificados, permisos, licencias, derechos administrativos, bonos, deuda pública, beneficios, trazabilidad presupuestaria, activos públicos tokenizados, comprobantes, registros o instrumentos de gestión pública.

Su emisión deberá respetar legalidad, transparencia, finalidad pública, protección de datos, prohibición de vigilancia masiva, auditoría pública, interoperabilidad y control institucional.

Ningún token público podrá utilizarse para implementar una CBDC de control social, censura económica, expiración arbitraria de beneficios, condicionamiento político, scoring social o vigilancia financiera indiscriminada.

Artículo 130. Tokens DeFi

Son tokens DeFi aquellos utilizados dentro de protocolos de finanzas descentralizadas, incluyendo tokens de liquidez, staking tokens, receipt tokens, governance tokens, collateral tokens, yield tokens, synthetic tokens, LP tokens y otros instrumentos programables.

Su clasificación dependerá de:

a) Función dentro del protocolo.
b) Derechos económicos incorporados.
c) Riesgo para usuarios.
d) Grado de descentralización del protocolo.
e) Existencia de emisor o administrador.
f) Custodia o no custodia.
g) Control efectivo sobre parámetros.
h) Promesa de rendimiento.
i) Dependencia de esfuerzos de terceros.
j) Acceso a liquidez o colateral.

Artículo 131. Tokens Sintéticos y Derivados Digitales

Son tokens sintéticos o derivados digitales aquellos que representan exposición económica a un activo, índice, precio, tasa, evento, commodity, divisa, activo digital, acción, instrumento financiero o variable externa, sin necesariamente conferir titularidad directa sobre el activo subyacente.

Estos activos estarán sujetos a supervisión reforzada cuando sean ofrecidos al público, impliquen apalancamiento, liquidaciones automatizadas, riesgo sistémico, contraparte identificable o exposición compleja.

La IID podrá establecer requisitos de idoneidad, divulgación, límites, margen, oráculos, auditoría y protección al usuario.

Artículo 132. Tokens de Privacidad

Son tokens de privacidad o activos digitales con funciones avanzadas de privacidad aquellos que incorporan mecanismos criptográficos para proteger información transaccional, identidad, saldos, montos, participantes o datos asociados.

La existencia de funciones de privacidad no constituirá por sí misma presunción de ilicitud.

Su uso legítimo estará protegido como parte de la privacidad financiera y la seguridad digital. Las obligaciones regulatorias deberán enfocarse en intermediarios, custodios, VASP y conductas ilícitas verificables, no en la mera existencia de tecnología de privacidad.

Artículo 133. Tokens de Infraestructura

Son tokens de infraestructura aquellos utilizados para operar, asegurar, incentivar, gobernar o acceder a redes descentralizadas, incluyendo tokens de gas, validación, staking técnico, almacenamiento, computación, ancho de banda, oráculos, seguridad, disponibilidad de datos o servicios descentralizados.

No serán considerados valores o instrumentos financieros por defecto cuando su función principal sea técnica u operativa dentro de una red.

Podrán ser sujetos a reglas especiales cuando sean comercializados predominantemente como inversión o cuando exista control centralizado, promesa de rendimiento o captación del público.

Artículo 134. Tokens Híbridos

Son tokens híbridos aquellos que combinan funciones de pago, utilidad, gobernanza, inversión, representación de activos reales, privacidad, infraestructura o derechos económicos.

Cuando un token tenga funciones múltiples, se aplicará el régimen correspondiente al componente de mayor riesgo, sin desconocer sus demás funciones legítimas ni imponer cargas desproporcionadas sobre usos no financieros.

La IID podrá emitir criterios de clasificación, guías interpretativas o resoluciones técnicas para determinar el régimen aplicable.

SECCIÓN III — REGLAS DE CALIFICACIÓN Y PREVENCIÓN DE ARBITRAJE REGULATORIO

Artículo 135. Sustancia sobre Forma

La clasificación de un activo digital se realizará conforme a su sustancia económica y jurídica, no únicamente conforme al nombre utilizado por sus emisores, promotores, plataformas o participantes.

No bastará denominar un token como utilidad, gobernanza, NFT, stablecoin, DeFi o descentralizado para evitar el régimen aplicable cuando su estructura real corresponda a inversión, custodia, captación, intermediación, derivado o servicio financiero.

Artículo 136. Descentralización Real y Control Efectivo

Para determinar la clasificación y régimen aplicable, la IID evaluará el grado de descentralización real y control efectivo sobre el activo, protocolo o ecosistema.

Se considerarán factores relevantes:

a) Existencia de emisor identificable.
b) Capacidad de modificar reglas.
c) Control de admin keys.
d) Capacidad de censurar usuarios.
e) Control de liquidez.
f) Control de oráculos.
g) Concentración de gobernanza.
h) Promesas públicas de rendimiento.
i) Control sobre tesorería.
j) Dependencia de un equipo promotor.
k) Capacidad de congelar o revertir transacciones.
l) Control de front-end esencial.
m) Custodia de activos de terceros.

Artículo 137. Régimen de Transición de Descentralización Progresiva

Los proyectos que nazcan con control inicial pero tengan una ruta verificable hacia descentralización podrán acogerse a un régimen de descentralización progresiva ante la IID.

Dicho régimen podrá incluir:

a) Plan público de descentralización.
b) Calendario de reducción de control.
c) Divulgación de admin keys.
d) Reglas de gobernanza.
e) Auditorías de smart contracts.
f) Límites a insiders.

g) Transparencia de tesorería.
h) Protección de usuarios.
i) Reportes periódicos.
j) Criterios de graduación hacia menor carga regulatoria.

Artículo 138. Prohibición de Simulación de Descentralización

Queda prohibido presentar como descentralizado un activo, plataforma, protocolo, token, DAO o servicio que conserve control centralizado relevante sin divulgarlo de forma clara.

La simulación de descentralización será considerada práctica engañosa y podrá generar responsabilidad administrativa, civil o penal según corresponda.

SECCIÓN IV — RELACIÓN CON VASP, AML/CFT Y ESTÁNDARES INTERNACIONALES

Artículo 139. Clasificación de Activos y Actividad VASP

La clasificación de un activo digital no determina por sí sola la existencia de actividad VASP.

La actividad VASP dependerá de la prestación profesional, habitual o empresarial de servicios sobre activos digitales por cuenta de terceros, incluyendo custodia, intercambio, transferencia, intermediación, administración, colocación, operación de plataformas o servicios equivalentes definidos por ley.

Los usuarios que actúen por cuenta propia, autocustodien activos, operen wallets no custodiales, transfieran peer-to-peer, participen en protocolos descentralizados o desarrollen software neutral no serán VASP por ese solo hecho.

Artículo 140. Aplicación de GAFI/FATF Recomendación 15

Costa Rica aplicará la Recomendación 15 de GAFI/FATF respecto de activos virtuales y VASP mediante un enfoque basado en riesgo, proporcionalidad, neutralidad tecnológica y respeto a derechos fundamentales.

La IID coordinará con las autoridades competentes para desarrollar reglas sobre:

a) Debida diligencia del cliente para VASP.
b) Monitoreo basado en riesgo.
c) Travel Rule entre VASP.
d) Reporte de operaciones sospechosas.
e) Sanciones proporcionales.
f) Cooperación internacional.
g) Supervisión de custodios e intermediarios.
h) Evaluación de riesgos sectoriales.
i) Prevención de abuso sin vigilancia masiva.
j) Protección de autocustodia legítima.

Artículo 141. Travel Rule/CARF Compatible con Autocustodia

Las obligaciones de intercambio de información en transferencias de activos digitales se aplicarán prioritariamente a transferencias entre VASP, custodios, intermediarios o sujetos obligados.

Las transferencias entre wallets no custodiales no serán tratadas automáticamente como operaciones VASP, salvo cuando exista intermediación profesional, custodia de terceros, actividad empresarial organizada o indicios verificables de ilicitud conforme a ley.

La IID deberá establecer estándares técnicos que permitan cumplimiento AML/CFT sin imponer vigilancia masiva, identificación obligatoria universal, prohibición de autocustodia o debilitamiento de privacidad financiera.

Artículo 142. Enfoque Basado en Riesgo y No Prohibición General

Ninguna categoría de activo digital podrá ser prohibida de forma general por su tecnología, descentralización, privacidad, volatilidad, transferibilidad o resistencia a censura.

Las restricciones deberán basarse en riesgos concretos, evidencia técnica, proporcionalidad, debido proceso y necesidad demostrada.

El Estado podrá sancionar conductas ilícitas, fraudes, abusos, intermediación no autorizada o incumplimientos regulatorios, sin criminalizar tecnologías neutrales o usos legítimos.

SECCIÓN V — COMPETENCIA DE LA IID EN CLASIFICACIÓN

Artículo 143. Autoridad de Clasificación

La IID será la autoridad técnica competente para emitir criterios de clasificación de activos digitales conforme a este capítulo, sin perjuicio de la coordinación con otras autoridades cuando existan implicaciones tributarias, penales, registrales, comerciales, de valores, consumo o AML/CFT.

La clasificación deberá realizarse mediante procedimientos transparentes, motivados, técnicamente fundados y sujetos a revisión.

Artículo 144. Registro Voluntario de Clasificación

La IID podrá establecer un mecanismo voluntario de consulta o registro de clasificación para emisores, desarrolladores, DAOs, VASP, proyectos, inversionistas institucionales o usuarios que requieran certeza jurídica sobre la categoría de un activo digital.

La respuesta de la IID deberá indicar:

a) Categoría aplicable.
b) Régimen jurídico principal.
c) Obligaciones de divulgación.
d) Riesgos regulatorios.
e) Obligaciones AML/CFT si corresponde.
f) Tratamiento de custodia o intermediación.
g) Condiciones para mantener la clasificación.

Artículo 145. Revisión y Actualización de Clasificación

La clasificación de un activo digital podrá revisarse cuando cambien sus características, gobernanza, derechos, grado de descentralización, forma de comercialización, reservas, control efectivo, uso dominante o riesgo sistémico.

La recalificación no tendrá efectos retroactivos sancionatorios salvo fraude, ocultamiento, mala fe o simulación.

SECCIÓN VI — CLÁUSULAS DE PROTECCIÓN DE INNOVACIÓN Y SOBERANÍA FINANCIERA

Artículo 146. Protección de Innovación Abierta

La clasificación de activos digitales deberá interpretarse de forma que preserve el desarrollo de redes abiertas, software libre, protocolos descentralizados, wallets no custodiales, identidad soberana, tokenización legítima, DeFi y participación peer-to-peer.

La regulación no podrá utilizarse para favorecer artificialmente al sistema financiero tradicional, imponer intermediación obligatoria, bloquear competencia descentralizada o impedir modelos tecnológicos legítimos.

Artículo 147. Cláusula Pro Autocustodia

Toda duda interpretativa sobre la clasificación de activos digitales deberá resolverse de forma compatible con el derecho a la autocustodia, salvo cuando exista custodia profesional de terceros, fraude, captación pública, intermediación regulada o riesgo concreto demostrado.

Artículo 148. Cláusula de Soberanía Financiera Digital

La clasificación de activos digitales en Costa Rica deberá proteger la capacidad de las personas de participar en redes económicas globales, acceder a activos digitales, utilizar Bitcoin, interactuar con protocolos, transferir valor, custodiar patrimonio propio y desarrollar innovación financiera sin discriminación tecnológica indebida.

Ninguna interpretación de este capítulo podrá utilizarse para imponer monopolios bancarios, vigilancia financiera masiva, CBDCs obligatorias, prohibición general de wallets no custodiales o exclusión arbitraria del ecosistema de tecnologías descentralizadas y emergentes.

Artículo 149. Cláusula Final de Clasificación Funcional

Las categorías establecidas en este capítulo constituyen la base taxativa del régimen costarricense de activos digitales.

Cualquier nueva categoría o subcategoría deberá crearse mediante ley o regulación técnica de la IID, bajo los principios de transparencia, consulta pública, neutralidad tecnológica, proporcionalidad, protección de derechos fundamentales, cumplimiento internacional y defensa de la innovación descentralizada.

CAPÍTULO V — INTEGRIDAD, CIBERSEGURIDAD Y GARANTÍAS TECNOLÓGICAS DEL SISTEMA ELECTORAL

SECCIÓN I — PRINCIPIOS DE INTEGRIDAD Y GARANTÍA TECNOLÓGICA ELECTORAL

Artículo 150. Integridad Electoral Digital

La digitalización de procesos electorales deberá preservar los principios constitucionales de pureza del sufragio, secreto del voto, autenticidad, integridad, disponibilidad, auditabilidad, accesibilidad, trazabilidad técnica y protección de datos.

Las disposiciones de este capítulo establecen garantías y estándares mínimos de resultado. Corresponderá a la autoridad electoral constitucionalmente competente definir, dentro de sus atribuciones exclusivas, la arquitectura, tecnologías, procedimientos y mecanismos concretos para su implementación.

Las materias relativas al financiamiento de partidos políticos, contribuciones, gastos, propaganda y control financiero electoral se regirán exclusivamente por la Constitución Política, el Código Electoral y la normativa dictada por la autoridad electoral competente.

Artículo 151. Supremacía del Voto Libre, Secreto, Igual, Directo y Verificable

Todo sistema electoral digital deberá preservar el carácter libre, secreto, igual, directo, universal y verificable del voto.

La digitalización electoral no podrá debilitar el secreto del sufragio, permitir coerción, identificar la preferencia política del votante, manipular resultados, discriminar electores, excluir poblaciones vulnerables o reducir garantías constitucionales.

La verificabilidad electoral deberá diseñarse de manera que permita comprobar la integridad del proceso sin revelar la identidad ni la decisión individual del votante, incluyéndose intrínsecamente Zero Knowledge Proof (ZKP).

Artículo 152. Autonomía de la Autoridad Electoral y Estándares de Seguridad Digital

La autoridad electoral constitucionalmente competente conservará íntegramente sus atribuciones exclusivas de organización, dirección y vigilancia de los actos relativos al sufragio.

Los estándares tecnológicos previstos en esta ley deberán interpretarse como garantías de integridad, seguridad, auditabilidad y protección de derechos, sin facultar a la IID, al MICITT ni a otra autoridad administrativa para avocar, sustituir, revisar o dirigir decisiones propias de la autoridad electoral.

Artículo 153. Garantismo Electoral Digital

Toda innovación tecnológica electoral deberá aplicarse bajo un enfoque garantista, orientado a ampliar derechos, fortalecer confianza pública, reducir fraude, mejorar accesibilidad, proteger privacidad y facilitar fiscalización.

No podrá implementarse tecnología electoral que:

Reduzca garantías existentes.
b) Aumente opacidad.
c) Genere dependencia tecnológica crítica.
d) Impida auditoría independiente.
e) Debilite el secreto del voto.
f) Excluya a personas por brecha digital.
g) Centralice indebidamente datos electorales.
h) Permita vigilancia política.
i) Sustituya revisión humana sin control.
j) Dependa de proveedores cerrados no auditables.

k) Exportación de datos sensibles de ciudadanos costarricenses, sus residentes y/o información de cualquier Institución Pública, del Gobierno Central, el descentralizado como Municipios, El Legislativo, Judicial, que interfiera con la seguridad nacional y la protección de datos sensibles.

SECCIÓN II — INFRAESTRUCTURA ELECTORAL SEGURA, AUDITABLE Y VERIFICABLE

Artículo 154. Registro Electoral Verificable

El registro electoral deberá contar con mecanismos digitales de integridad, trazabilidad y verificación pública que permitan auditar su consistencia, actualización, cambios, exclusiones, inclusiones y modificaciones sin exponer datos personales sensibles.

El Estado podrá utilizar blockchain, hashes, sellos de tiempo, pruebas criptográficas, credenciales verificables y registros distribuidos para anclar la integridad del padrón electoral y sus modificaciones.

La ciudadanía, partidos políticos, observadores, universidades y órganos de control deberán contar con mecanismos adecuados para verificar que el registro electoral no ha sido manipulado, alterado o depurado de forma indebida.

Artículo 155. Auditoría Tecnológica de Procesos Electorales

La autoridad electoral podrá utilizar registros distribuidos, hashes, sellos de tiempo, pruebas criptográficas u otras tecnologías equivalentes como mecanismos de integridad y verificación cuando técnicamente resulten apropiados.

Toda solución deberá ser auditable, interoperable y compatible con el secreto del voto, la protección de datos, la accesibilidad, la continuidad operativa y el control público conforme al ordenamiento electoral. Esta ley no impone una tecnología específica ni sustituye la competencia técnica y constitucional de la autoridad electoral.

Artículo 156. Prohibición de Sistemas Electorales de Caja Negra

Queda prohibida la utilización de sistemas electorales digitales cuyo funcionamiento, código, arquitectura, criterios de decisión, mecanismos de conteo, transmisión, almacenamiento o auditoría no puedan ser examinados por autoridades competentes, partidos políticos, observadores técnicos independientes y ciudadanía bajo condiciones razonables de seguridad.

No podrán invocarse secretos comerciales, propiedad intelectual, seguridad nacional o confidencialidad contractual para impedir la auditoría de sistemas electorales que afecten derechos políticos fundamentales.

Todo proveedor tecnológico electoral deberá aceptar auditoría técnica, revisión de código, pruebas de penetración, evaluación de seguridad, documentación completa y mecanismos de verificación independiente.

Artículo 157. Código Abierto, Auditoría Independiente y Revisión Pública

El software electoral de relevancia crítica deberá tender progresivamente hacia estándares de código abierto, documentación pública, reproducibilidad, auditoría independiente y revisión técnica plural.

Cuando razones excepcionales impidan publicación completa del código, la autoridad electoral constitucionalmente competente deberá justificarlo de forma motivada y permitir auditoría técnica suficiente por universidades, expertos independientes, partidos políticos, organizaciones especializadas y órganos de control.

La auditoría deberá realizarse antes, durante y después del proceso electoral, incluyendo pruebas de integridad, seguridad, reproducibilidad, resistencia a manipulación y verificación de resultados.

Artículo 158. Descentralización de Infraestructura Electoral Crítica

La infraestructura tecnológica electoral deberá diseñarse para evitar puntos únicos de falla, dependencia de proveedores únicos, control centralizado excesivo, vulnerabilidades sistémicas, captura corporativa, interferencia extranjera y manipulación interna, que pongan en riesgo la seguridad nacional.

El autoridad electoral constitucionalmente competente deberá implementar mecanismos de redundancia, replicación segura, copias verificables, auditoría distribuida, custodia institucional de llaves, registros inmutables y planes de continuidad operativa.

Cuando sea técnicamente viable, se fomentará la descentralización de componentes de verificación electoral mediante nodos institucionales, académicos, ciudadanos o partidarios, sin comprometer el secreto del voto ni la autoridad final dla autoridad electoral constitucionalmente competente.

SECCIÓN III — IDENTIDAD ELECTORAL SOBERANA Y PROTECCIÓN DEL VOTO

Artículo 159. Identidad Electoral Soberana

La identidad electoral digital deberá diseñarse bajo principios de soberanía personal, privacidad, minimización de datos, interoperabilidad, seguridad, verificabilidad y control ciudadano.

La identidad electoral digital no podrá convertirse en identidad digital universal obligatoria para toda la vida civil, financiera, social o política de la persona.

Su uso deberá limitarse a finalidades electorales específicas, sin permitir vigilancia política, perfilamiento ideológico, seguimiento de participación cívica o integración masiva con bases de datos no electorales, phone home, control ciudadano, debiendo más bien prevalecer la “prueba de cero conocimiento- Zero Knowledge Proof- ZKP”.

Artículo 160. Secreto del Voto y Privacidad Criptográfica

Todo sistema electoral digital deberá garantizar que ninguna autoridad, proveedor, partido político, observador, tercero o sistema automatizado pueda vincular la identidad de una persona con su voto.

La privacidad electoral podrá protegerse mediante mecanismos criptográficos avanzados, incluyendo pruebas de conocimiento cero, credenciales verificables, cifrado extremo a extremo, separación de identidad y voto, mixnets, firmas ciegas u otras tecnologías equivalentes, con el mayor estándar de ciberseguridad posible.

La ley deberá asegurar que la verificabilidad del voto no vulnere su secreto.

Artículo 161. Prohibición de Trazabilidad Personal del Voto

Queda prohibido cualquier sistema, base de datos, token, credencial, blockchain, identificador digital, dispositivo, algoritmo o mecanismo técnico que permita rastrear, inferir, reconstruir o vincular la preferencia electoral de una persona determinada.

La trazabilidad electoral solo podrá referirse al proceso, documentos, actas, transmisión, conteo, auditorías y resultados, nunca a la decisión individual del elector.

La violación de esta prohibición será considerada lesión grave al orden constitucional democrático.

Artículo 162. Accesibilidad Electoral Digital

La digitalización electoral deberá garantizar accesibilidad, inclusión y no discriminación para personas adultas mayores, personas con discapacidad, poblaciones rurales, comunidades indígenas, personas con baja alfabetización digital, ciudadanos en el exterior y cualquier grupo en situación de vulnerabilidad.

Ninguna innovación electoral digital podrá excluir o dificultar irrazonablemente el ejercicio del sufragio por razones tecnológicas, económicas, territoriales, lingüísticas o de conectividad.

SECCIÓN IV — COORDINACIÓN TÉCNICA Y RESPETO DE LA AUTONOMÍA ELECTORAL

Artículo 163. Coordinación Técnica en Infraestructura Electoral Digital

La IID podrá prestar asistencia técnica, emitir recomendaciones no vinculantes y compartir alertas de ciberseguridad o vulnerabilidades con la autoridad electoral, cuando esta lo solicite o cuando se identifique un riesgo técnico grave que pueda afectar infraestructura electoral digital.

La coordinación se realizará mediante protocolos que respeten la autonomía, reserva funcional y competencias exclusivas de la autoridad electoral. La IID no ejercerá potestad sancionatoria, de auditoría coercitiva, dirección, avocación o sustitución respecto de actos relativos al sufragio.

Artículo 164. Auditoría Técnica Obligatoria

Todo sistema electoral digital crítico deberá someterse a auditorías técnicas obligatorias, independientes y documentadas.

Estas auditorías deberán evaluar, como mínimo:

Seguridad informática.
b) Integridad del software.
c) Protección contra manipulación.
d) Gestión de llaves criptográficas.
e) Protección de datos personales.
f) Resiliencia operativa.
g) Dependencia tecnológica.
h) Riesgos de proveedor.
i) Vulnerabilidades conocidas.
j) Trazabilidad de cambios.
k) Reproducibilidad de resultados.

l) Cumplimiento de secreto del voto.
m) Riesgo de vigilancia o perfilamiento.

o) Riesgo de exportación de datos sensibles de ciudadanos o de la Institución en sí misma, que ponga en riesgo la seguridad nacional del país.

Los informes deberán ser públicos en la mayor medida posible, salvo información estrictamente sensible cuya reserva deberá justificarse y someterse a control independiente.

Artículo 165. Fiscalización Ciudadana, Partidaria y Académica

Los partidos políticos, ciudadanía, universidades, colegios profesionales, organizaciones de sociedad civil, expertos técnicos y observadores independientes tendrán derecho a participar en mecanismos razonables de fiscalización de sistemas electorales digitales.

El autoridad electoral constitucionalmente competente deberá establecer canales de revisión, pruebas públicas, reportes de vulnerabilidades, observación técnica, acceso documentado, auditorías externas y mecanismos de verificación post-electoral.

La fiscalización técnica deberá realizarse bajo reglas de seguridad, responsabilidad, confidencialidad proporcional y protección de la integridad del proceso.

Artículo 166. Garantías de Legalidad y Control de Infraestructura Electoral Digital

Toda infraestructura tecnológica utilizada en procesos electorales deberá respetar la Constitución Política, el Código Electoral, los derechos fundamentales y los principios de seguridad, auditabilidad, secreto, transparencia y trazabilidad aplicables.

El control de legalidad, constitucionalidad y jurisdicción electoral corresponderá a las autoridades competentes conforme al ordenamiento. Ninguna disposición de esta ley podrá interpretarse como transferencia de competencias electorales a la IID o al MICITT.

SECCIÓN V — PROHIBICIONES ELECTORALES DIGITALES

Artículo 167. Manipulación Algorítmica, Propaganda Digital y Remisión al Régimen Electoral

Queda prohibido utilizar sistemas automatizados, inteligencia artificial, deepfakes, bots coordinados, suplantación digital u otras tecnologías para ejecutar conductas ilícitas de manipulación, fraude, falsedad o interferencia en procesos electorales, en los términos definidos por la legislación electoral y penal aplicable.

La regulación sustantiva del financiamiento de partidos políticos, contribuciones, gastos, propaganda electoral, deberes de reporte y controles financieros se regirá exclusivamente por el artículo 96 de la Constitución Política, el Código Electoral y la normativa emitida por la autoridad electoral competente.

Las disposiciones de esta ley se limitarán a estándares tecnológicos de autenticidad, ciberseguridad, identificación de contenido sintético y preservación de evidencia, sin modificar los procedimientos ni controles constitucionalmente reservados al régimen electoral.

Artículo 168. Prohibición de Proveedores Tecnológicos Electorales Opacos

El Estado no podrá contratar proveedores tecnológicos electorales que se nieguen a auditorías, revisión de código, documentación técnica, trazabilidad, pruebas de seguridad, controles de dependencia, transferencia de conocimiento o mecanismos de verificación independiente.

Todo contrato tecnológico electoral deberá incluir cláusulas de:

a) Auditoría.
b) Reversibilidad.
c) Portabilidad.
d) Seguridad.
e) Continuidad operativa.
f) Soberanía de datos.
g) Prohibición de explotación secundaria de datos.
h) Transparencia de subcontratistas.
i) Responsabilidad por fallas.
j) Cooperación con fiscalización pública.

Artículo 169. Prohibición de Identidad Electoral Centralizada con Fines de Vigilancia

Queda prohibido crear sistemas de identidad electoral centralizada que permitan seguimiento político, perfilamiento ideológico, trazabilidad de participación, monitoreo de preferencias, discriminación partidaria o integración indebida con bases de datos financieras, policiales, migratorias, sanitarias, educativas, comerciales o de telecomunicaciones.

La identidad electoral digital deberá limitarse estrictamente a verificar elegibilidad y participación, sin exponer ni inferir preferencias políticas.

Artículo 170. Prohibición de Voto Digital sin Verificabilidad Independiente

No podrá implementarse voto electrónico, voto remoto, voto por internet o cualquier modalidad digital de emisión de sufragio si no existe verificabilidad independiente, auditoría técnica suficiente, garantía del secreto del voto, resiliencia, accesibilidad, trazabilidad del proceso y mecanismos de impugnación.

La digitalización del voto deberá adoptarse únicamente cuando demuestre ser igual o más garantista que los mecanismos tradicionales.

Artículo 171. Prohibición de Blockchain Electoral Mal Diseñada

Queda prohibido utilizar blockchain electoral de forma que exponga identidad del votante, permita reconstruir preferencias, centralice control en pocos nodos, genere vigilancia política, impida corrección legal, debilite secreto del voto o cree falsa sensación de seguridad.

La tecnología blockchain deberá utilizarse únicamente cuando aumente integridad, verificabilidad, trazabilidad institucional y confianza pública sin afectar derechos fundamentales.

SECCIÓN VI — SOBERANÍA ELECTORAL DIGITAL

Artículo 172. Soberanía Electoral Tecnológica

La infraestructura electoral digital será considerada infraestructura crítica de soberanía nacional.

Su diseño, operación, auditoría, custodia de datos, gestión de llaves, proveedores, almacenamiento, transmisión, respaldo y verificación deberán estar sometidos a controles reforzados de soberanía, seguridad, transparencia e independencia institucional.

No podrá depender de gobiernos extranjeros, proveedores opacos, nubes no auditables, sistemas cerrados, contratos incompatibles con auditoría pública o infraestructuras que comprometan la independencia electoral costarricense.

Artículo 173. Gestión Criptográfica Electoral

Toda infraestructura electoral que utilice criptografía, blockchain, firmas digitales, credenciales verificables o sistemas de cifrado deberá contar con reglas estrictas de generación, custodia, rotación, recuperación, auditoría y destrucción de llaves criptográficas.

La gestión de llaves no podrá concentrarse en una sola persona, proveedor, partido, funcionario o entidad sin controles de multifirma, separación de funciones, trazabilidad y auditoría independiente.

Artículo 174. Archivo Electoral Digital Inmutable

Los documentos electorales críticos deberán conservarse mediante mecanismos de archivo digital seguro, trazable, verificable e inmutable, sin perjuicio de rectificaciones legales debidamente registradas.

El archivo electoral digital deberá incluir, según corresponda:

Actas.
b) Resoluciones.
c) Escrutinios.
d) Impugnaciones.
e) Auditorías.
f) Reportes técnicos.
g) Contratos tecnológicos.
h) Publicación de resultados.
i) Evidencia de transmisión.
j) Hashes de sistemas y documentos relevantes.

k) Control de cambios y funcionario responsable.

Artículo 175. Observatorio Nacional de Integridad Electoral Digital

Créase o habilítase un mecanismo nacional de observación técnica de integridad electoral digital, integrado por perfiles técnicos, jurídicos, académicos, cívicos y de ciberseguridad, con participación plural y no partidista.

Su función será emitir recomendaciones, auditar riesgos, revisar tecnologías emergentes, evaluar amenazas digitales, proponer estándares y fortalecer la confianza pública en procesos electorales digitales.

Dicho mecanismo no sustituirá al autoridad electoral constitucionalmente competente ni interferirá con sus competencias exclusivas, pero servirá como órgano técnico consultivo y de fiscalización ciudadana especializada.

Artículo 176. Cláusula de Supremacía Democrática Digital

Toda infraestructura, tecnología, contrato, algoritmo, sistema de identidad, base de datos, blockchain, mecanismo de voto, transmisión de resultados o herramienta digital utilizada en materia electoral deberá interpretarse conforme al principio de supremacía democrática digital.

Será contrario a este principio todo sistema que:

Debilite el secreto del voto.
b) Impida auditoría independiente.
c) Centralice indebidamente control tecnológico.
d) Exponga datos electorales personales.
e) Cree dependencia crítica de proveedores.
f) Use cajas negras algorítmicas.
g) Permita manipulación de resultados.
h) Impida fiscalización ciudadana.

i) Genere vigilancia política.
j) Sustituya confianza democrática por confianza ciega en tecnología.

k) Utilice phone home.

CAPÍTULO VI — IDENTIDAD DIGITAL SOBERANA, PRIVACIDAD Y DERECHOS CRIPTOGRÁFICOS

SECCIÓN I — PRINCIPIOS DE IDENTIDAD DIGITAL SOBERANA

Artículo 177. Reconocimiento Legal de la Identidad Digital Soberana

Toda persona tiene derecho al reconocimiento, protección, control, portabilidad, seguridad y soberanía sobre su identidad digital.

La identidad digital comprende identificadores, credenciales, llaves criptográficas, firmas digitales, atributos verificables, datos personales, reputación digital, representaciones electrónicas, historial de interacción, permisos, certificaciones y cualquier mecanismo que permita acreditar existencia, voluntad, capacidad, titularidad, reputación o participación en entornos digitales.

Ninguna autoridad pública o entidad privada podrá apropiarse, centralizar, condicionar, suspender, explotar o transferir la identidad digital de una persona sin base legal expresa, consentimiento válido o resolución motivada conforme al debido proceso.

Artículo 178. Derecho a la Identidad Autosoberana

Toda persona tiene derecho a utilizar sistemas de identidad autosoberana que le permitan controlar sus credenciales, atributos, llaves, pruebas de identidad y mecanismos de autenticación sin dependencia obligatoria de un proveedor único, plataforma centralizada, banco, institución pública o tercero privado.

El Estado promoverá estándares de self-sovereign identity, identificadores descentralizados, credenciales verificables, interoperabilidad abierta, minimización de datos y privacidad por diseño.

La identidad autosoberana no podrá utilizarse para evadir responsabilidades legales, suplantar identidad, cometer fraude o impedir investigaciones legítimas; pero tampoco podrá ser prohibida por su naturaleza descentralizada.

Artículo 179. Derecho a Credenciales Verificables

Toda persona tiene derecho a recibir, portar, presentar, verificar y revocar credenciales digitales verificables emitidas por autoridades públicas, entidades privadas, universidades, colegios profesionales, instituciones financieras, sistemas de salud, organizaciones civiles o redes descentralizadas.

Las credenciales verificables deberán diseñarse para revelar únicamente la información necesaria para una finalidad determinada, evitando exposición excesiva de datos personales.

Podrán utilizarse para acreditar, entre otros:

a) Identidad.
b) Mayoría de edad.
c) Residencia.
d) Capacidad legal.
e) Titulación académica.
f) Licencias profesionales.
g) Permisos administrativos.
h) Certificaciones laborales.

i) Elegibilidad electoral.
j) Cumplimiento regulatorio.
k) Titularidad patrimonial.
l) Reputación técnica o profesional.

Artículo 180. Separación entre Identidad y Vigilancia

La identidad digital no podrá diseñarse ni utilizarse como mecanismo de vigilancia permanente, seguimiento conductual, rastreo financiero, monitoreo político, perfilamiento ideológico, scoring social o control automatizado de acceso a derechos.

Todo sistema de identidad digital deberá separar estrictamente:

a) Verificación de identidad.
b) Autenticación.
c) Autorización.
d) Registro de actividad.
e) Perfilamiento.
f) Monitoreo.
g) Analítica de comportamiento.

La verificación legítima de identidad no autoriza trazabilidad generalizada de la vida digital de una persona.

SECCIÓN II — PROTECCIÓN CRIPTOGRÁFICA Y PRIVACIDAD

Artículo 181. Derecho al Uso de Criptografía

Toda persona tiene derecho a utilizar criptografía para proteger identidad, comunicaciones, datos, activos digitales, wallets, credenciales, documentos, transacciones, propiedad digital, dispositivos, registros y participación en entornos digitales.

Queda prohibido imponer puertas traseras, debilitamiento obligatorio del cifrado, acceso secreto masivo, escaneo indiscriminado o vulnerabilidades deliberadas en sistemas criptográficos utilizados lícitamente.

Las limitaciones deberán ser excepcionales, individualizadas, proporcionales, previstas por ley y sujetas a control judicial o autoridad competente.

Artículo 182. Protección de Zero Knowledge Proofs

El Estado reconocerá las pruebas de conocimiento cero y demás mecanismos criptográficos de divulgación selectiva como herramientas legítimas para verificar atributos, cumplimiento, identidad, edad, elegibilidad, solvencia, residencia, titularidad, límites regulatorios o condiciones legales sin revelar información innecesaria.

Ninguna autoridad podrá rechazar un mecanismo criptográfico de prueba únicamente porque preserve privacidad, siempre que permita verificar de forma segura el atributo o condición requerida.

El Estado promoverá el uso de ZKP cuando permita cumplir objetivos regulatorios sin exponer datos personales o financieros.

Artículo 183. Derecho al Pseudonimato y Anonimato Legítimo

Toda persona tiene derecho al uso de pseudónimos, identificadores descentralizados, wallets, llaves criptográficas, credenciales selectivas y mecanismos de privacidad en entornos digitales lícitos.

El anonimato o pseudonimato legítimo será especialmente protegido cuando resguarde libertad de expresión, seguridad personal, privacidad financiera, participación política, defensa de derechos, periodismo, investigación, innovación, protección de denunciantes o participación en redes descentralizadas.

Este derecho no ampara fraude, suplantación de identidad, lavado de dinero, financiamiento ilícito, explotación de personas, extorsión, terrorismo ni conductas tipificadas como delito.

Artículo 184. Protección contra Identificación Masiva

Queda prohibida la identificación digital masiva, indiscriminada o permanente de personas en espacios físicos o digitales mediante biometría, reconocimiento facial, análisis de comportamiento, geolocalización, metadatos, rastreo de dispositivos, actividad financiera o patrones de navegación.

La identificación digital solo podrá realizarse con finalidad específica, base legal, proporcionalidad, minimización de datos, temporalidad, seguridad y mecanismos de impugnación.

SECCIÓN III — PROTECCIÓN BIOMÉTRICA Y DATOS SENSIBLES

Artículo 185. Protección Legal Reforzada de Datos Biométricos

Los datos biométricos y las plantillas derivadas de características físicas, fisiológicas o conductuales de una persona serán considerados datos sensibles sujetos a protección legal reforzada, de conformidad con la Constitución Política y la legislación de protección de datos personales.

Su tratamiento deberá observar necesidad, finalidad específica, minimización, seguridad, proporcionalidad, retención limitada y mecanismos de impugnación. Cuando sea técnicamente viable, deberán preferirse arquitecturas de verificación local, credenciales verificables, pruebas de conocimiento cero u otras técnicas que eviten la concentración innecesaria de bases biométricas.

El acceso administrativo a documentos privados o bases de datos protegidas por el artículo 24 de la Constitución Política solo procederá conforme a las habilitaciones y garantías constitucionales y legales aplicables.

Artículo 186. Prohibición de Biometría Obligatoria Generalizada

Queda prohibida la imposición generalizada de biometría como condición universal para acceder a servicios públicos, internet, economía digital, servicios financieros, educación, salud, transporte, trabajo, participación política o infraestructura tecnológica.

La biometría solo podrá utilizarse cuando sea estrictamente necesaria, no exista alternativa menos invasiva, se garantice protección reforzada y no genere exclusión, vigilancia o discriminación.

Artículo 187. Prohibición de Integración Masiva de Datos

Queda prohibida la integración indiscriminada de datos biométricos, financieros, electorales, sanitarios, fiscales, migratorios, educativos, laborales, judiciales, comerciales, de telecomunicaciones o identidad digital que permita construir perfiles totales de las personas.

La interoperabilidad deberá limitarse a finalidades específicas, autorizadas, proporcionales y auditables.

SECCIÓN IV — INFRAESTRUCTURA DE IDENTIDAD SOBERANA

Artículo 188. Identificadores Descentralizados y Credenciales Descentralizadas

El Estado reconocerá los identificadores descentralizados y las credenciales verificables como mecanismos válidos para autenticar, acreditar, verificar y portar identidad o atributos digitales.

Su implementación deberá respetar estándares abiertos, interoperabilidad, seguridad, revocabilidad, portabilidad, control individual, minimización de datos y privacidad por diseño.

Artículo 189. Interoperabilidad sin Centralización

Los sistemas de identidad digital deberán interoperar sin crear dependencia obligatoria de un único registro, proveedor, wallet, plataforma, banco, nube, blockchain o autoridad centralizada.

La interoperabilidad no podrá justificar vigilancia, perfilamiento, concentración de datos o pérdida de control individual.

Artículo 190. Portabilidad, Revocación y Recuperación

Toda persona tendrá derecho a portar sus credenciales digitales, revocar permisos, actualizar atributos, corregir información, recuperar acceso bajo mecanismos seguros y migrar entre proveedores o wallets compatibles.

Los sistemas deberán prever mecanismos de recuperación que no eliminen soberanía individual ni creen puntos únicos de control.

Artículo 191. Infraestructura Nacional de Identidad Soberana

Costa Rica podrá desarrollar una infraestructura nacional de identidad digital soberana basada en estándares abiertos, credenciales verificables, privacidad por diseño, ZKP, descentralización progresiva, interoperabilidad y control individual.

Dicha infraestructura será voluntaria, garantista, auditable, no discriminatoria y no podrá convertirse en requisito universal para ejercer derechos, acceder a internet, participar en la economía digital o utilizar servicios privados.

SECCIÓN V — LÍMITES CONSTITUCIONALES A LA IDENTIDAD DIGITAL

Artículo 192. Prohibición de Scoring Social

Queda prohibido todo sistema público o privado de scoring social obligatorio que clasifique personas para otorgar o restringir derechos, servicios, oportunidades, movilidad, crédito, empleo, participación política o acceso digital con base en comportamiento, ideología, reputación, actividad financiera, historial digital o asociaciones personales.

Artículo 193. Prohibición de Identidad Digital Obligatoria Universal

El Estado no podrá imponer una identidad digital única, centralizada y obligatoria como condición general para existir, comunicarse, navegar, expresarse, pagar, invertir, estudiar, trabajar, votar, contratar o participar en la economía digital.

Podrán existir mecanismos de identificación para finalidades legítimas específicas, pero no una arquitectura universal de rastreo.

Artículo 194. Prohibición de Vigilancia Conductual

Queda prohibido utilizar identidad digital, credenciales, wallets, biometría, datos financieros, navegación, geolocalización o interacciones digitales para vigilancia conductual generalizada de la población.

La analítica pública deberá limitarse a finalidades legítimas, agregadas, anonimizadas cuando sea posible, proporcionales y no discriminatorias.

Artículo 195. Cláusula de Dignidad Digital

Toda política, sistema, ley, contrato, plataforma o infraestructura relacionada con identidad digital deberá interpretarse conforme a la dignidad humana, la autonomía individual, la privacidad, la libertad financiera, el debido proceso, la minimización de datos y el control soberano de la persona sobre su vida digital.

Será contrario a este marco todo sistema que convierta la identidad digital en mecanismo de vigilancia, exclusión, coerción, censura, discriminación, control financiero o subordinación tecnológica.

CAPÍTULO VII — TOKENIZACIÓN DE LA ECONOMÍA Y ACTIVOS DEL MUNDO REAL

SECCIÓN I — PRINCIPIOS GENERALES DE TOKENIZACIÓN

Artículo 196. Reconocimiento Jurídico de la Tokenización

El Estado reconoce la tokenización como mecanismo jurídico-tecnológico válido para representar, transmitir, fraccionar, registrar, verificar, custodiar, gravar, financiar o ejecutar derechos sobre activos digitales, físicos, financieros, contractuales, públicos o privados.

La tokenización podrá utilizarse para activos del mundo real, instrumentos financieros, bienes inmuebles, participaciones corporativas, derechos económicos, propiedad intelectual, activos ambientales, infraestructura, deuda, commodities, facturas, créditos, garantías, certificados y demás bienes o derechos permitidos por ley.

Artículo 197. Principio de Equivalencia Funcional

La representación tokenizada de un derecho, activo u obligación tendrá validez jurídica cuando cumpla los requisitos sustantivos y formales aplicables al derecho subyacente.

La forma digital, criptográfica o tokenizada de representación no disminuirá por sí sola la protección jurídica del titular ni la exigibilidad del derecho representado.

La tokenización no altera la naturaleza jurídica del activo subyacente salvo disposición legal expresa; únicamente modifica su forma tecnológica de representación, trazabilidad, transferencia, fraccionamiento, liquidación o verificación. Cuando el ordenamiento exija escritura pública, inscripción registral, autorización administrativa, consentimiento de terceros u otra formalidad constitutiva, el token no sustituirá por sí solo tales requisitos.

Artículo 198. Tokenización como Infraestructura Económica Nacional

La tokenización será considerada infraestructura estratégica para modernizar la economía costarricense, facilitar inversión, ampliar mercados, fortalecer trazabilidad productiva, reducir intermediación innecesaria, mejorar liquidez y conectar activos nacionales con redes financieras globales.

El Estado promoverá la tokenización bajo principios de:

a) Seguridad jurídica.
b) Transparencia.
c) Trazabilidad.
d) Interoperabilidad.
e) Neutralidad tecnológica.
f) Protección del inversionista.
g) Autocustodia legítima.
h) Prevención de fraude.
i) Cumplimiento proporcional.
j) Acceso inclusivo a mercados.
k) Respeto a la propiedad privada.
l) Protección de datos y privacidad.

SECCIÓN II — ACTIVOS TOKENIZABLES

Artículo 199. Bienes Inmuebles Tokenizados

Los bienes inmuebles, derechos reales, derechos posesorios, desarrollos inmobiliarios, fideicomisos inmobiliarios, participaciones sobre proyectos, usufructos, servidumbres, arrendamientos, garantías hipotecarias y demás derechos inmobiliarios podrán ser tokenizados conforme a la ley.

La tokenización inmobiliaria deberá garantizar:

a) Identificación precisa del inmueble o derecho.
b) Titularidad verificable.
c) Relación con Registro Público y Catastro.
d) Determinación clara de derechos del token holder.
e) Existencia de contratos soporte.
f) Régimen de copropiedad o participación.
g) Reglas de transferencia.
h) Tratamiento de gravámenes.
i) Mecanismos de ejecución.
j) Prevención de doble tokenización.
k) Divulgación de riesgos.
l) Cumplimiento tributario y registral cuando corresponda.

Artículo 200. Tokenización Corporativa

Podrán tokenizarse acciones, participaciones sociales, cuotas, derechos económicos, instrumentos convertibles, derechos de voto, derechos de suscripción, deuda corporativa, ingresos futuros y otros instrumentos societarios permitidos por ley.

La tokenización corporativa deberá respetar:

a) Estatutos sociales.
b) Libros societarios.
c) Derechos de accionistas o socios.
d) Restricciones de transferencia.
e) Pactos parasociales.
f) Normativa de valores cuando aplique.
g) Derechos de información.
h) Reglas de gobernanza.
i) Protección de minorías.
j) Transparencia sobre dilución, beneficios y riesgos.

La tokenización no podrá utilizarse para evadir responsabilidades societarias, ocultar beneficiarios finales, defraudar socios o realizar ofertas públicas encubiertas.

Artículo 201. Tokenización Agrícola, Productiva y Exportadora

Costa Rica promoverá la tokenización de activos agrícolas, cosechas, inventarios, contratos de compra futura, exportaciones, créditos productivos, trazabilidad de origen, certificaciones de calidad, cadenas de suministro, financiamiento rural y activos vinculados a la producción nacional.

Podrán tokenizarse, entre otros:

a) Cosechas futuras.
b) Inventarios agrícolas.
c) Derechos sobre producción.
d) Contratos de exportación.
e) Certificaciones de origen.
f) Créditos agrícolas.
g) Facturas comerciales.
h) Receivables.
i) Activos logísticos.

j) Trazabilidad de productos.
k) Garantías productivas.

La tokenización productiva deberá fortalecer acceso a financiamiento, transparencia de cadenas de suministro, inclusión de pequeños productores, competitividad exportadora y trazabilidad internacional.

Artículo 202. Tokenización Energética y Ambiental

Podrán tokenizarse activos energéticos, créditos ambientales, certificados de carbono, bonos verdes, energía renovable, proyectos de conservación, biodiversidad, servicios ecosistémicos, agua, reforestación, impacto climático y otros instrumentos ambientales permitidos por ley.

La tokenización ambiental deberá garantizar:

a) Existencia verificable del activo ambiental.
b) Metodologías reconocidas.
c) Prevención de doble conteo.
d) Auditoría independiente.
e) Trazabilidad del impacto.
f) Transparencia de beneficiarios.
g) Protección contra greenwashing.
h) Cumplimiento con estándares nacionales e internacionales.
i) Respeto a comunidades locales e indígenas cuando corresponda.

Artículo 203. Propiedad Intelectual Tokenizada

Podrán tokenizarse derechos de propiedad intelectual, derechos de autor, regalías, licencias, marcas, patentes, software, obras artísticas, música, audiovisuales, diseños, secretos empresariales protegidos, derechos editoriales y otros activos intangibles.

La tokenización deberá definir claramente:

a) Derecho tokenizado.
b) Titular del derecho.
c) Alcance de licencia o propiedad.
d) Duración.
e) Territorio.
f) Regalías.
g) Restricciones de uso.
h) Derechos morales cuando apliquen.
i) Mecanismos de ejecución.
j) Relación con registros de propiedad intelectual.

Artículo 203 bis. Activo digital estratégico descentralizado

Bitcoin podrá ser reconocido como activo digital estratégico descentralizado por su grado de descentralización, seguridad de red, interoperabilidad global, resistencia a censura, liquidez internacional y relevancia geoeconómica, sin que ello implique reconocimiento como moneda de curso legal, obligación de aceptación, sustitución del colón costarricense o afectación de competencias del Banco Central de Costa Rica.

El reconocimiento estratégico de Bitcoin no autoriza sustitución monetaria, emisión de deuda encubierta, política cambiaria paralela, captación pública no autorizada ni utilización obligatoria por personas físicas, jurídicas, comercios o instituciones públicas.

Artículo 203 ter. Reserva digital estratégica

La IID, en coordinación con el Banco Central de Costa Rica, el Ministerio de Hacienda, MICITT y demás autoridades competentes, podrá elaborar estudios técnicos sobre la viabilidad, riesgos, condiciones prudenciales y límites jurídicos de una reserva digital estratégica.

La eventual creación de una reserva digital estratégica requerirá ley especial, análisis de impacto fiscal, autorización presupuestaria, mecanismos de custodia institucional, criterios de riesgo, transparencia reforzada, control de legalidad, auditoría y protección del interés público.

Artículo 204. Activos Públicos Tokenizados

El Estado podrá tokenizar activos públicos, derechos económicos, proyectos de infraestructura, deuda pública, concesiones, certificados, bonos verdes, instrumentos ambientales, derechos de uso o participaciones económicas únicamente cuando su naturaleza jurídica permita dicha representación y exista habilitación legal suficiente.

Toda tokenización pública deberá someterse a: a) legalidad estricta; b) transparencia presupuestaria; c) control de la Contraloría cuando corresponda; d) auditoría externa; e) trazabilidad de fondos; f) aprobación legislativa cuando sea exigible; g) protección de datos; h) prevención de opacidad fiscal; i) publicidad de condiciones; y j) prohibición de vigilancia financiera.

La tokenización no modificará la naturaleza demanial o de dominio público de los bienes, ni habilitará su enajenación, gravamen, concesión o transferencia cuando el ordenamiento exija autorización especial. Tampoco podrá utilizarse para evadir límites de endeudamiento, controles presupuestarios, contratación pública o responsabilidad fiscal.

SECCIÓN III — INTEGRIDAD JURÍDICA, REGISTRO Y ACTIVO SUBYACENTE

Artículo 204 bis. Tokenización Pública e Infraestructuras de Mercado Digital

La tokenización de activos públicos, fondos estatales, instrumentos financieros públicos o patrimonios soberanos estratégicos solo podrá desarrollarse mediante habilitación legal, autorización de las autoridades competentes, análisis fiscal, supervisión institucional, transparencia, auditoría, control presupuestario y protección del interés público.

La IID podrá coordinar estudios técnicos, pilotos controlados, lineamientos preliminares y recomendaciones de política pública para sistemas de negociación autorizados, mercados secundarios regulados, liquidación digital, tokenización pública y plataformas de infraestructura económica digital.

La presente disposición no crea una bolsa única, monopolio, exclusividad ni reserva estatal de actividad. Toda infraestructura de mercado de activos digitales deberá respetar integridad de mercado, prevención de abuso, protección de usuarios, interoperabilidad financiera, supervisión competente, trazabilidad proporcional y estándares internacionales aplicables.

Artículo 205. Relación entre Token y Activo Subyacente

Todo activo tokenizado deberá establecer de forma clara, verificable y jurídicamente exigible la relación entre el token y el activo, derecho u obligación subyacente.

El documento de tokenización deberá indicar:

a) Naturaleza del activo subyacente.
b) Titularidad.
c) Derechos conferidos por el token.
d) Limitaciones.
e) Reglas de transferencia.
f) Mecanismos de redención o ejecución.

g) Riesgos.
h) Custodia o administración del activo.
i) Derechos frente al emisor o administrador.
j) Ley aplicable.
k) Jurisdicción o mecanismos de resolución de disputas.

Artículo 206. Prevención de Doble Tokenización y Doble Gravamen

Queda prohibida la doble tokenización fraudulenta de un mismo activo, derecho u obligación, así como la emisión de tokens que representen derechos incompatibles, inexistentes, duplicados o no autorizados sobre un mismo subyacente.

Los sistemas de tokenización deberán incluir mecanismos para verificar:

a) Unicidad del activo.
b) Gravámenes existentes.
c) Restricciones legales.
d) Tokens previamente emitidos.
e) Capacidad del emisor.
f) Titularidad legítima.
g) Registro o anotación cuando corresponda.
h) Auditoría del subyacente.

Artículo 207. Integración con Registro Público Blockchain

Cuando el activo tokenizado esté sujeto a registro público, catastro, registro mercantil, registro de propiedad intelectual, registro de garantías, registro ambiental u otro registro oficial, la tokenización deberá interoperar con dichos sistemas en la medida aplicable.

La integración podrá realizarse mediante:

a) Anclaje criptográfico.
b) Hashes.
c) Certificados verificables.
d) Smart contracts registrales.
e) APIs públicas.
f) Identificadores únicos.
g) Sellos de tiempo.
h) Notificación registral.
i) Mecanismos de oposición o bloqueo legal.

Artículo 208. Smart Contracts Ejecutables

Los smart contracts utilizados para tokenización podrán automatizar transferencia, liquidación, reparto de ingresos, derechos de voto, pago de regalías, garantías, redención, condiciones de cumplimiento, restricciones de transferencia y eventos contractuales.

Su utilización deberá garantizar:

a) Auditoría técnica.
b) Documentación jurídica.
c) Correspondencia entre código y contrato legal.
d) Mecanismos de corrección ante error.
e) Gestión de contingencias.
f) Protección de usuarios.

g) Resolución de disputas.
h) Seguridad de llaves.
i) Transparencia de reglas.
j) Cumplimiento normativo aplicable.

SECCIÓN IV — COPROPIEDAD TOKENIZADA, FRACCIONALIZACIÓN Y MERCADOS DIGITALES

Artículo 209. Copropiedad y Fraccionamiento Tokenizado

Los activos podrán ser fraccionados mediante tokens cuando la ley permita copropiedad, participación económica, derechos proporcionales, unidades de inversión, cuotas, derechos de uso, derechos sobre ingresos o estructuras equivalentes.

El fraccionamiento deberá definir:

a) Derechos de cada titular.
b) Derechos de voto o decisión.
c) Participación en ingresos.
d) Obligaciones de mantenimiento.
e) Restricciones de transferencia.
f) Administración del activo.
g) Régimen de salida.
h) Resolución de conflictos.
i) Tratamiento de insolvencia.
j) Ejecución frente a terceros.

Artículo 210. Mercados Secundarios de Activos Tokenizados

Los activos tokenizados podrán negociarse en mercados secundarios, plataformas autorizadas, protocolos descentralizados o mecanismos privados, conforme a su clasificación jurídica, nivel de riesgo y régimen aplicable.

Cuando el activo tokenizado tenga naturaleza de inversión, valor, deuda, participación colectiva o instrumento financiero, su mercado secundario deberá cumplir reglas de transparencia, protección del inversionista, prevención de manipulación, divulgación de riesgos y supervisión proporcional.

La negociación peer-to-peer de activos propios no constituirá por sí misma operación de mercado regulado, salvo actividad profesional habitual, intermediación, custodia o plataforma organizada.

Artículo 211. Custodia, Proof of Reserves y Proof of Assets

Cuando exista custodio, administrador, emisor, fiduciario, plataforma o tercero responsable de activos tokenizados o reservas subyacentes, deberá implementarse un régimen de transparencia proporcional que podrá incluir:

a) Proof of reserves.
b) Proof of assets.
c) Auditoría externa.
d) Verificación de titularidad.
e) Informes periódicos.
f) Separación patrimonial.
g) Controles de custodia.
h) Gestión de llaves.
i) Cobertura de riesgos.
j) Divulgación de pasivos relacionados.

La IID establecerá estándares técnicos diferenciados según tipo de activo, riesgo y grado de intermediación.

SECCIÓN V — TRANSPARENCIA, PROTECCIÓN Y PREVENCIÓN DE FRAUDE

Artículo 212. Documento de Divulgación de Activos Tokenizados

Toda oferta pública o dirigida a múltiples inversionistas de activos tokenizados deberá contar con un documento de divulgación claro, suficiente y no engañoso.

El documento deberá incluir, según corresponda:

a) Descripción del activo.
b) Derechos conferidos.
c) Riesgos.
d) Titularidad del subyacente.
e) Método de valoración.
f) Régimen de transferencia.
g) Costos y comisiones.
h) Información del emisor o administrador.
i) Custodia.
j) Auditoría.
k) Gobernanza.
l) Tributación general aplicable.
m) Conflictos de interés.
n) Smart contracts utilizados.
o) Mecanismos de reclamación.

Artículo 213. Auditoría de Tokenización

Los proyectos de tokenización deberán someterse a auditoría proporcional cuando involucren oferta pública, activos de terceros, activos públicos, reservas, fraccionamiento masivo, instrumentos financieros, fondos administrados o relevancia sistémica.

La auditoría podrá comprender:

a) Existencia del activo subyacente.
b) Titularidad.
c) Valuación.
d) Gravámenes.
e) Contratos soporte.
f) Smart contracts.
g) Seguridad informática.
h) Cumplimiento regulatorio.
i) Separación patrimonial.
j) Riesgos de liquidez.
k) Protección de inversionistas.
l) Riesgo de doble emisión.

Artículo 214. Protección contra Fraude Tokenizado

Quedan prohibidas las siguientes conductas:

a) Tokenizar activos inexistentes.
b) Representar derechos no autorizados.
c) Duplicar tokens sobre el mismo activo.
d) Ocultar gravámenes relevantes.

e) Falsear reservas.
f) Manipular precios.
g) Simular respaldo jurídico.
h) Vender utilidad como inversión sin disclosure.
i) Prometer rendimientos inexistentes.
j) Ocultar conflictos de interés.
k) Usar tokenización para evadir controles legales.
l) Crear estructuras destinadas a defraudar inversionistas o acreedores.

SECCIÓN VI — SOBERANÍA ECONÓMICA TOKENIZADA

Artículo 215. Costa Rica como Hub de Tokenización

El Estado promoverá a Costa Rica como jurisdicción líder en tokenización de activos reales, economía digital, infraestructura blockchain, derechos digitales, identidad soberana, activos ambientales, economía productiva, inversión internacional y mercados Web3/Web4.

Para ello, podrá impulsar:

a) Sandboxes regulatorios.
b) Guías técnicas de tokenización.
c) Integración con Registro Público blockchain.
d) Incentivos a innovación responsable.
e) Educación técnica y jurídica.
f) Reconocimiento internacional.
g) Cooperación con universidades.
h) Atracción de inversión extranjera.
i) Estándares de certificación.
j) Plataformas interoperables.
k) Programas de exportación digital.

Artículo 216. Neutralidad Tecnológica y Competencia en Tokenización

La tokenización podrá implementarse sobre distintas redes, protocolos, blockchains, capas de interoperabilidad, infraestructuras públicas, privadas, híbridas o descentralizadas, siempre que cumplan estándares de seguridad, trazabilidad, integridad, protección de derechos y cumplimiento normativo.

El Estado no deberá imponer una red única ni favorecer monopolios tecnológicos.

Artículo 217. Cláusula de Soberanía Económica Digital

Toda política pública relacionada con tokenización deberá interpretarse conforme a la soberanía económica digital de Costa Rica, la libertad financiera, la propiedad privada, la innovación abierta, la protección del inversionista, la transparencia del Estado, la autocustodia, la interoperabilidad y la prevención de vigilancia masiva.

Será contrario a este marco cualquier modelo de tokenización que:

a) Imponga intermediación obligatoria innecesaria.
b) Genere dependencia tecnológica crítica.
c) Oculte activos públicos.
d) Debilite propiedad privada.
e) Facilite vigilancia financiera.
f) Simule respaldo inexistente.
g) Excluya a pequeños participantes.

h) Capture mercados mediante monopolios.
i) Eluda controles constitucionales.
j) Convierta la tokenización en CBDC encubierta.

CAPÍTULO VIII — MERCADOS DE ACTIVOS DIGITALES, INFRAESTRUCTURA FINANCIERA DESCENTRALIZADA Y BANCA DIGITAL SOBERANA

SECCIÓN I — MERCADOS SECUNDARIOS DE ACTIVOS DIGITALES

Artículo 218. Reconocimiento de Mercados Secundarios Tokenizados

El Estado reconoce la existencia y legitimidad de mercados secundarios para activos digitales, activos tokenizados, instrumentos financieros tokenizados, RWA, stablecoins, Bitcoin, tokens de utilidad, tokens de gobernanza, tokens DeFi, NFTs financieros y demás activos digitales permitidos por ley.

Los mercados secundarios podrán operar mediante:

a) Bolsas de activos digitales.
b) Plataformas de negociación autorizadas.
c) Sistemas alternativos de trading Web3.
d) Exchanges centralizados.
e) Protocolos descentralizados.
f) Mercados peer-to-peer.
g) Mercados institucionales tokenizados.
h) Infraestructura híbrida TradFi-Web3.

La regulación aplicable dependerá de la naturaleza del activo, el tipo de mercado, la existencia de custodia, el nivel de intermediación, el acceso al público, el riesgo sistémico y el grado de control efectivo.

Artículo 219. Operadores de Mercados y Bolsas de Activos Digitales

Créase la categoría regulatoria de operadores de mercados o bolsas de activos digitales. Podrán existir uno o varios operadores autorizados por la IID bajo condiciones objetivas, transparentes, proporcionales y no discriminatorias.

La autorización estará sujeta a requisitos de gobernanza, integridad de mercado, ciberseguridad, segregación y custodia cuando corresponda, transparencia, prevención de conflictos de interés, continuidad operativa, protección del usuario y demás condiciones definidas por esta ley.

La presente disposición no crea monopolio, exclusividad, concesión única ni reserva estatal de actividad. Los instrumentos que, por su naturaleza jurídica, se encuentren sometidos a un régimen especial distinto conservarán las competencias y requisitos que correspondan conforme a la legislación sectorial aplicable.

Artículo 220. Sistemas Alternativos de Trading Web3

La IID podrá autorizar Sistemas Alternativos de Trading Web3 para la negociación organizada de activos digitales, activos tokenizados, RWA, instrumentos privados, tokens de inversión y otros activos permitidos.

Estos sistemas podrán operar bajo modelos:

a) Institucionales.
b) Minoristas.
c) Profesionales.
d) Privados.
e) Descentralizados con front-end autorizado.

f) Híbridos con liquidación on-chain.
g) Especializados por tipo de activo.

Los Sistemas Alternativos de Trading Web3 deberán contar con reglas claras de acceso, listado, negociación, divulgación, custodia, liquidación, resolución de disputas, prevención de manipulación y gestión de riesgos.

Artículo 221. Mercados Descentralizados y DEX

Los mercados descentralizados, DEX, automated market makers, order books on-chain, liquidity pools y protocolos de intercambio descentralizado serán reconocidos como infraestructura legítima de negociación de activos digitales.

No serán considerados bolsas, intermediarios o VASP por su mera existencia técnica cuando operen sin custodia, sin control centralizado, sin administración discrecional y sin entidad que controle fondos de usuarios.

Cuando exista front-end administrado, control de acceso, custodia, comisiones centralizadas, capacidad de censura, modificación unilateral, control de liquidez u operación empresarial identificable, la IID podrá imponer obligaciones proporcionales al grado de control efectivo.

Artículo 222. Listado de Activos Digitales

Toda plataforma autorizada que liste activos digitales deberá aplicar procesos de evaluación proporcional según la categoría del activo.

La evaluación podrá incluir:

a) Clasificación jurídica del activo.
b) Riesgos tecnológicos.
c) Liquidez.
d) Existencia o inexistencia de emisor.
e) Nivel de descentralización.
f) Riesgos de mercado.
g) Riesgos de smart contract.
h) Riesgos de oráculos.
i) Riesgos de reservas o colateral.
j) Información disponible al público.
k) Historial de seguridad.
l) Riesgos AML/CFT.
m) Conflictos de interés.

La IID podrá establecer reglas diferenciadas para listado de Bitcoin, stablecoins, tokens RWA, security tokens, tokens DeFi y activos de alto riesgo.

SECCIÓN II — INFRAESTRUCTURA DE LIQUIDACIÓN BLOCKCHAIN

Artículo 223. Settlement On-Chain

El Estado reconoce la validez de la liquidación de operaciones mediante blockchain, registros distribuidos, smart contracts, stablecoins, activos digitales, tokens de liquidación, sistemas de pago blockchain y mecanismos criptográficos equivalentes.

La liquidación on-chain podrá ser utilizada para:

a) Compraventa de activos digitales.
b) Liquidación de activos tokenizados.
c) Pagos de valores tokenizados.
d) Liquidación contra entrega.

e) Entrega contra pago.
f) Pagos transfronterizos.
g) Colateralización.
h) Ejecución de garantías.
i) Liquidación de mercados secundarios.
j) Operaciones institucionales.

La liquidación on-chain tendrá efectos jurídicos cuando cumpla requisitos de autenticidad, integridad, consentimiento, trazabilidad, finalización y cumplimiento normativo aplicable.

Artículo 224. Finalidad de Liquidación Digital

Las operaciones liquidadas mediante blockchain podrán adquirir finalidad jurídica cuando se cumplan las condiciones técnicas y contractuales establecidas por la plataforma, smart contract, protocolo o normativa aplicable.

La finalidad de liquidación digital deberá proteger:

a) Seguridad jurídica de las partes.
b) Irrevocabilidad técnica cuando corresponda.
c) Corrección legal en caso de fraude o error judicialmente reconocido.
d) Integridad del registro.
e) Protección frente a doble gasto.
f) Compatibilidad con insolvencia.
g) Evidencia criptográfica verificable.

Artículo 225. Custodia Opcional y Autocustodia en Mercados

Los mercados de activos digitales deberán permitir, cuando sea técnicamente viable y compatible con la naturaleza del servicio, modelos de negociación con autocustodia, custodia segregada, custodia institucional, custodia programable o custodia híbrida.

La participación en mercados digitales no deberá exigir obligatoriamente la entrega de activos a un custodio centralizado cuando existan mecanismos seguros de liquidación no custodial.

Las plataformas que ofrezcan custodia deberán separar activos propios y de clientes, mantener controles de llaves, proof of reserves, auditoría externa, seguros cuando corresponda y reglas claras de insolvencia.

Artículo 226. Proof of Reserves, Proof of Liabilities y Transparencia Financiera

Las entidades que utilicen blockchain, DLT o infraestructura digital nativa para prestar servicios bancarios o financieros estarán sujetas a la legislación bancaria, monetaria y prudencial cuando capten recursos del público, realicen intermediación financiera o ejecuten actividades legalmente reservadas.

La utilización de tecnología blockchain-native no alterará por sí sola la naturaleza jurídica de la actividad ni permitirá eludir las competencias del Banco Central de Costa Rica, CONASSIF, SUGEF u otras autoridades competentes.

La IID ejercerá sus competencias únicamente sobre la capa de activos digitales, infraestructura Web3 y mercados digitales que esta ley le atribuya, mediante coordinación institucional y sin duplicidad regulatoria.

Artículo 227. Clearing y Liquidación Tokenizada

La IID podrá autorizar cámaras de compensación, sistemas de clearing, smart contracts de liquidación, protocolos de netting, sistemas de margen, garantías tokenizadas y mecanismos de gestión de riesgo para mercados digitales.

Estos sistemas deberán garantizar:

a) Transparencia operativa.
b) Gestión de riesgo.
c) Liquidación eficiente.
d) Protección de colateral.
e) Auditoría de smart contracts.
f) Reglas ante incumplimiento.
g) Resiliencia.
h) Gobernanza.
i) Interoperabilidad.
j) Protección frente a riesgo sistémico.

SECCIÓN III — BANCA DIGITAL SOBERANA Y BANCOS BLOCKCHAIN-NATIVE

Artículo 228. Reconocimiento de Bancos Digitales Blockchain-Native

El Estado reconoce la figura de bancos digitales blockchain-native como entidades autorizadas para prestar servicios financieros basados en blockchain, activos digitales, stablecoins, tokenización, custodia opcional, pagos digitales, liquidación on-chain, crédito tokenizado y servicios financieros programables.

Estos bancos podrán operar bajo autorización especializada, supervisión proporcional y estándares diferenciados respecto de la banca tradicional, siempre que cumplan reglas de solvencia, transparencia, protección de usuarios, AML/CFT, ciberseguridad, gobernanza y separación de riesgos.

Artículo 229. Bancos de Activos Digitales

Los bancos de activos digitales podrán prestar servicios de:

a) Custodia de activos digitales.
b) Cuentas de activos digitales.
c) Pagos blockchain.
d) Liquidación stablecoin.
e) Crédito con colateral tokenizado.
f) Tokenización de activos.
g) Servicios de emisión.
h) Infraestructura de mercado.
i) Staking institucional cuando sea permitido.
j) Gestión de tesorería digital.
k) Proof of reserves.
l) Servicios fiduciarios digitales.

Estos servicios deberán distinguir claramente entre custodia, depósito, inversión, crédito, pagos, staking, administración y autocustodia asistida.

Artículo 230. Reservas Verificables On-Chain

Las entidades financieras digitales que emitan instrumentos respaldados, stablecoins, saldos tokenizados, productos de custodia o activos representativos deberán mantener reservas verificables conforme a estándares definidos por la IID.

Las reservas podrán verificarse mediante:

a) Auditorías externas.
b) Proof of reserves.
c) Proof of liabilities.

d) Reportes on-chain.
e) Cuentas segregadas.
f) Certificaciones bancarias.
g) Smart contracts de colateral.
h) Oráculos auditados.
i) Reportes periódicos públicos.

Artículo 231. Stablecoin Banking

Los bancos digitales, bancos tradicionales autorizados, emisores especializados y entidades blockchain-native podrán prestar servicios vinculados a stablecoins bajo reglas de reservas, redención, transparencia, ciberseguridad, protección de usuarios y prevención de riesgo sistémico.

Las stablecoins no serán depósitos bancarios por defecto, pero cuando una entidad ofrezca instrumentos equivalentes a depósitos, deberá cumplir requisitos específicos de solvencia, reservas, protección al usuario y divulgación.

Artículo 232. Banca DeFi Híbrida

La IID podrá autorizar modelos de banca DeFi híbrida que integren servicios financieros tradicionales con protocolos descentralizados, smart contracts, stablecoins, colateral tokenizado, mercados automatizados y liquidación on-chain.

Estos modelos deberán cumplir con:

a) Transparencia de riesgos.
b) Identificación de protocolos utilizados.
c) Auditoría de smart contracts.
d) Gestión de colateral.
e) Protección de usuarios.
f) Separación entre activos propios y de clientes.
g) Gobernanza de riesgos.
h) Controles AML/CFT proporcionales.
i) Pruebas de estrés.
j) Planes de contingencia.

Artículo 233. Separación de Custodia, Crédito y Riesgo

Toda entidad financiera digital deberá separar claramente las funciones de custodia, intermediación, crédito, inversión, staking, pagos, liquidación y administración de activos.

Los activos en custodia deberán mantenerse segregados del patrimonio de la entidad y no podrán ser prestados, invertidos, pignorados o utilizados sin autorización expresa del cliente y divulgación clara de riesgos.

SECCIÓN IV — INTEGRACIÓN ENTRE TRADFI Y WEB3

Artículo 234. Interoperabilidad Financiera

La infraestructura financiera tradicional y la infraestructura Web3 podrán interoperar mediante estándares abiertos, APIs, stablecoins, tokenización, sistemas de pago, banca abierta, identidad soberana, pruebas criptográficas, oráculos y liquidación blockchain.

La interoperabilidad deberá preservar:

a) Autocustodia.
b) Privacidad financiera.

c) Competencia.
d) Neutralidad tecnológica.
e) Protección de datos.
f) Ciberseguridad.
g) Cumplimiento proporcional.
h) Libertad de elección del usuario.

Artículo 235. Integración Bancaria Opcional

La participación en la economía digital no requerirá obligatoriamente integración bancaria, cuenta bancaria, custodio autorizado o intermediario financiero tradicional.

Los usuarios podrán interactuar directamente con activos digitales, wallets no custodiales, Bitcoin, stablecoins y protocolos descentralizados, sin perjuicio de las obligaciones aplicables a proveedores profesionales de servicios.

Artículo 236. Protección contra Debanking

Queda prohibida la exclusión bancaria arbitraria de personas físicas o jurídicas por realizar actividades lícitas relacionadas con activos digitales, blockchain, tokenización, Bitcoin, DeFi, stablecoins, wallets no custodiales, minería, validación, desarrollo de software o infraestructura Web3.

Las entidades financieras deberán basar sus decisiones en análisis individual de riesgo, conducta verificable y cumplimiento normativo, no en políticas generales de exclusión por sector.

Toda negativa, cierre o restricción deberá ser comunicada, motivada y sujeta a mecanismos de revisión.

SECCIÓN V — INFRAESTRUCTURA DE PAGOS BLOCKCHAIN

Artículo 237. Pagos Blockchain y Liquidación Instantánea

El Estado reconoce la validez de pagos realizados mediante Bitcoin, stablecoins, tokens de pago, activos digitales, smart contracts, wallets no custodiales y redes blockchain, siempre que las partes los acepten voluntariamente y no contravengan la ley.

Los pagos blockchain podrán utilizarse para comercio, remesas, servicios profesionales, comercio electrónico, turismo, exportaciones, micropagos, liquidación empresarial y pagos transfronterizos.

Artículo 238. Remesas y Pagos Internacionales

Costa Rica promoverá el uso de infraestructura blockchain, stablecoins, Bitcoin y sistemas de liquidación digital para reducir costos de remesas, pagos internacionales, comercio exterior, freelancers, turismo médico, exportaciones, servicios digitales y economía global.

Los proveedores profesionales deberán cumplir reglas proporcionales de transparencia, protección al usuario, AML/CFT y divulgación de riesgos.

Artículo 239. Micropagos y Economía Digital

El Estado promoverá infraestructura de micropagos digitales, streaming payments, pagos máquina-a-máquina, pagos por contenido, economía de creadores, IA, IoT, gaming, educación digital y servicios descentralizados.

Estos sistemas deberán proteger privacidad, consentimiento, transparencia de tarifas, reversibilidad cuando corresponda y seguridad de usuarios.

SECCIÓN VI — INTEGRIDAD DE MERCADO, SUPERVISIÓN Y PROTECCIÓN DEL USUARIO

Artículo 240. Integridad de Mercados Digitales

Los mercados de activos digitales deberán operar bajo reglas de integridad, transparencia, acceso equitativo, divulgación de información, prevención de manipulación, gestión de conflictos de interés, ciberseguridad y protección de usuarios.

La IID podrá dictar normas sobre:

a) Listado.
b) Delisting.
c) Market making.
d) Conflictos de interés.
e) Información privilegiada.
f) Manipulación de precios.
g) Wash trading.
h) Front-running.
i) Oracle manipulation.
j) Rug pulls.
k) Seguridad de smart contracts.
l) Controles de liquidez.

Artículo 241. Prevención de Manipulación y Abuso

Quedan prohibidas las prácticas de manipulación en mercados digitales, incluyendo wash trading, spoofing, pump and dump, uso indebido de información privilegiada, manipulación de oráculos, ataques coordinados, falsificación de volumen, front-running abusivo, rug pulls fraudulentos y difusión maliciosa de información falsa.

La IID deberá distinguir entre manipulación fraudulenta, volatilidad natural, actividad descentralizada legítima y fallas técnicas no dolosas.

Artículo 242. Protección del Usuario en Mercados Digitales

Las plataformas, bolsas, bancos digitales, custodios y proveedores regulados deberán proteger a usuarios mediante:

a) Divulgación clara de riesgos.
b) Transparencia de tarifas.
c) Seguridad de cuentas.
d) Segregación de activos.
e) Procedimientos de reclamo.
f) Educación financiera digital.
g) Prevención de publicidad engañosa.
h) Mecanismos de recuperación cuando sea posible.
i) Gestión de conflictos de interés.
j) Reportes de incidentes.

La protección del usuario no podrá utilizarse como pretexto para prohibir autocustodia o interacción directa con protocolos.

Artículo 243. Supervisión Proporcional de la IID

La IID supervisará mercados digitales, bolsas, VASP, bancos digitales blockchain-native, custodios, emisores, plataformas de tokenización y operadores con control efectivo mediante un enfoque proporcional, basado en riesgo, actividad, custodia, volumen, impacto, público objetivo y relevancia sistémica.

La supervisión deberá evitar:

a) Sobrerregulación.
b) Captura bancaria.
c) Barreras artificiales de entrada.
d) Monopolios de licencias.
e) Exclusión de startups.
f) Tratamiento igual para riesgos desiguales.
g) Criminalización de software neutral.
h) Eliminación de autocustodia.

SECCIÓN VII — SOBERANÍA FINANCIERA DIGITAL

Artículo 244. Costa Rica como Hub Financiero Web3

Costa Rica promoverá su posicionamiento como jurisdicción líder en mercados de activos digitales, tokenización, banca digital soberana, DeFi institucional, infraestructura de pagos blockchain, stablecoins, Bitcoin, RWA, identidad soberana y servicios financieros Web3/Web4.

Para ello podrá desarrollar:

a) Sandboxes regulatorios.
b) Pasarelas de reconocimiento internacional.
c) Incentivos a innovación responsable.
d) Educación técnica.
e) Infraestructura pública blockchain.
f) Certificaciones regulatorias.
g) Convenios internacionales.
h) Atracción de inversión.
i) Marcos fiscales competitivos.
j) Alianzas con universidades y sector privado.

Artículo 245. Competencia e Innovación Abierta

La regulación de mercados digitales deberá promover competencia, innovación abierta, interoperabilidad, nuevos entrantes, descentralización, neutralidad tecnológica y diversidad de modelos de negocio.

Queda prohibido utilizar licencias, infraestructura, acceso bancario, estándares técnicos o cumplimiento normativo como barreras artificiales para favorecer incumbentes, bancos, plataformas dominantes o monopolios tecnológicos.

Artículo 246. Cláusula de Soberanía Financiera Digital

Toda norma, autorización, supervisión o política pública relacionada con mercados de activos digitales, bancos digitales, bolsas, stablecoins, tokenización, pagos blockchain o infraestructura financiera descentralizada deberá interpretarse conforme a la soberanía financiera digital de las personas y de Costa Rica.

Será contrario a este marco todo diseño que:

a) Elimine autocustodia.
b) Imponga intermediación obligatoria innecesaria.
c) Cree dependencia de bancos tradicionales.
d) Habilite vigilancia financiera masiva.
e) Favorezca monopolios tecnológicos.
f) Bloquee mercados secundarios legítimos.
g) Impida liquidación on-chain.

h) Restrinja Bitcoin sin causa legítima.
i) Capture DeFi bajo categorías bancarias incompatibles.
j) Convierta innovación financiera en permiso permanente.

SECCIÓN FINAL — INFRAESTRUCTURA FINANCIERA DIGITAL INSTITUCIONAL, AML/KYT Y INFRAESTRUCTURAS DE LIQUIDACIÓN DE LIQUIDACIÓN

Artículo 247. Infraestructura Financiera Digital Institucional

El Estado costarricense promoverá el desarrollo de una infraestructura financiera digital interoperable, resiliente, compatible con estándares internacionales y tecnológicamente neutral, capaz de integrar sistemas bancarios tradicionales, activos digitales, stablecoins, tokenización, settlement on-chain, pagos digitales y servicios financieros descentralizados dentro de un marco de soberanía digital, estabilidad sistémica e integridad financiera.

La infraestructura financiera digital nacional deberá procurar: a) interoperabilidad bancaria; b) compatibilidad con sistemas de pagos nacionales e internacionales; c) resiliencia operativa; d) trazabilidad institucional legítima; e) protección al usuario; f) continuidad operacional; g) supervisión basada en riesgo; h) integración tecnológica abierta; i) neutralidad tecnológica; j) compatibilidad con estándares internacionales de compliance y liquidación.

Costa Rica no promoverá modelos de desregulación financiera opaca incompatibles con integridad financiera internacional, prevención de legitimación de capitales, estabilidad sistémica o cooperación transfronteriza.

Artículo 248. Supervisión AML/KYT Basada en Riesgo y Monitoreo Blockchain

Los proveedores de servicios de activos digitales, custodios, emisores de stablecoins, plataformas de tokenización, mercados digitales, proveedores OTC y demás actores regulados deberán implementar sistemas proporcionales de prevención de legitimación de capitales, financiamiento al terrorismo, financiamiento de proliferación y monitoreo de riesgo digital compatibles con estándares internacionales aplicables.

Dichos sistemas podrán incluir: a) KYC; b) KYT; c) monitoreo blockchain; d) análisis de riesgo transaccional; e) screening de wallets; f) monitoreo de exposición ilícita; g) detección de patrones anómalos; h) análisis de riesgo geográfico; i) Travel Rule cuando corresponda; j) monitoreo basado en riesgo sistémico.

La supervisión deberá respetar simultáneamente derechos fundamentales, proporcionalidad, privacidad legítima, autocustodia responsable, neutralidad tecnológica, debido proceso y prohibición de vigilancia masiva indiscriminada.

Artículo 249. Supervisión de Stablecoins y Riesgo Sistémico Digital

La IID podrá emitir regulación prudencial y estándares técnicos aplicables a stablecoins utilizadas de manera significativa dentro del ecosistema financiero digital costarricense.

La supervisión podrá contemplar: a) proof of reserves; b) auditorías independientes; c) segregación patrimonial; d) liquidez suficiente; e) mecanismos de redención; f) gestión de riesgo operativo; g) transparencia de respaldo; h) monitoreo de concentración; i) gestión de riesgo sistémico; j) interoperabilidad con infraestructura financiera nacional e internacional.

La regulación deberá diferenciar razonablemente entre stablecoins de pago, stablecoins respaldadas por activos, stablecoins algorítmicas, depósitos tokenizados y mecanismos híbridos de liquidación digital.

Artículo 250. Interoperabilidad Bancaria, APIs Financieras y Rails Fiat-Digitales

La infraestructura financiera digital costarricense deberá promover interoperabilidad entre sistemas bancarios, plataformas de activos digitales, proveedores de pagos, infraestructura de liquidación basada en stablecoins, APIs

financieras, sistemas de settlement on-chain, depósitos tokenizados, sistemas de identidad digital interoperable, infraestructuras de cumplimiento regulatorio y sistemas de pagos nacionales e internacionales.

La interoperabilidad podrá contemplar compatibilidad con ISO 20022, open banking, open finance, sistemas de liquidación digital, smart contracts financieros, infraestructura bancaria nacional y protocolos internacionales interoperables.

Ningún mecanismo de interoperabilidad podrá utilizarse para imponer vigilancia financiera masiva, bloqueo arbitrario de autocustodia legítima o exclusión financiera incompatible con derechos fundamentales.

Artículo 251. Estándares de Onboarding Institucional y Gobernanza Operacional

Los actores institucionales que operen infraestructura financiera digital relevante deberán implementar estándares razonables de gobernanza, onboarding institucional, debida diligencia y gestión de riesgo operacional compatibles con el nivel de riesgo de sus actividades.

La IID podrá emitir lineamientos sobre verificación de beneficiarios finales, source of funds, source of wealth, governance frameworks, segregación patrimonial, auditorías financieras y tecnológicas, gestión de riesgos, controles de ciberseguridad, continuidad operacional, custodia institucional y gestión de llaves criptográficas.

La regulación deberá mantener proporcionalidad razonable según tamaño, volumen, riesgo sistémico y naturaleza de cada actividad.

Artículo 252. Infraestructura OTC, Liquidez Digital y Tesorería Institucional

La IID podrá regular actividades relacionadas con provisión institucional de liquidez digital, operaciones OTC, market making, treasury digital, settlement institucional y servicios financieros digitales de gran escala cuando ello resulte necesario para proteger integridad de mercado, estabilidad sistémica y transparencia operacional.

Podrán establecerse estándares relacionados con gestión de liquidez, monitoreo de concentración, segregación de activos, controles de contraparte, reconciliación operacional, continuidad financiera, gestión de riesgo de mercado, trazabilidad institucional, gobernanza treasury y resiliencia operativa.

La regulación deberá evitar barreras desproporcionadas incompatibles con innovación legítima y competencia tecnológica.

Artículo 253. Custodia Institucional, Continuidad Operacional y Seguridad Financiera Digital

Las entidades que custodien activos digitales de terceros, operen infraestructura crítica financiera digital o administren sistemas relevantes de liquidación deberán implementar controles robustos de segregación patrimonial, gobernanza de llaves criptográficas, multifirma cuando corresponda, recuperación ante incidentes, continuidad operacional, respaldo de información, monitoreo de riesgos, ciberseguridad, resiliencia tecnológica y auditoría independiente.

La IID podrá exigir medidas reforzadas respecto de custodios sistémicos, stablecoins de uso masivo, infraestructura cloud crítica o sistemas relevantes para estabilidad financiera nacional.

Artículo 254. Salvaguardas Contra Arbitraje Regulatorio y Protección de Integridad Financiera Internacional

Costa Rica promoverá innovación financiera digital, interoperabilidad internacional y desarrollo tecnológico compatible con estándares globales de transparencia, integridad financiera y cooperación regulatoria.

La presente ley no podrá interpretarse como autorización para arbitraje regulatorio abusivo, ocultamiento de beneficiarios finales, estructuras opacas incompatibles con supervisión legítima, evasión sistemática de obligaciones AML/CFT, debilitamiento deliberado de cooperación internacional, utilización ilícita de infraestructura digital costarricense o evasión masiva mediante estructuras tecnológicas artificiosas.

La IID deberá promover cooperación internacional basada en supervisión proporcional, intercambio legítimo de información, protección de derechos fundamentales, interoperabilidad financiera responsable, estabilidad sistémica, soberanía digital e innovación compatible con integridad financiera global.

CAPÍTULO IX — GOVERNANCE DIGITAL, AUTOCUSTODIA RESPONSABLE Y COMPLIANCE CRIPTOGRÁFICO

SECCIÓN I — PRINCIPIOS DE AUTOCUSTODIA RESPONSABLE

Artículo 255. Reconocimiento de la Autocustodia Responsable

La autocustodia será reconocida como el derecho de toda persona a poseer, controlar, administrar y transferir activos digitales propios mediante wallets no custodiales, llaves privadas, hardware wallets, multisignature wallets, smart contracts u otras herramientas criptográficas lícitas.

La autocustodia responsable implica la obligación ética, técnica y jurídica de evitar el uso de infraestructura descentralizada para fraude, lavado de dinero, financiamiento ilícito, evasión deliberada de sanciones, abuso de mercado, ocultamiento de origen ilícito o contaminación intencional de liquidez.

La mera autocustodia no convertirá a una persona en sujeto obligado, VASP, custodio, intermediario financiero o entidad regulada.

Artículo 256. Integridad Transaccional Voluntaria

Las personas que utilicen autocustodia podrán adoptar mecanismos voluntarios de integridad transaccional para demostrar, ante mercados, contrapartes, plataformas, bancos digitales, protocolos institucionales o autoridades competentes, que sus fondos no presentan exposición relevante a actividades ilícitas.

Dichos mecanismos podrán incluir:

a) Certificaciones criptográficas.
b) Pruebas de origen razonable de fondos.
c) Análisis de exposición a sanciones.
d) Attestations emitidas por terceros independientes.
e) Credenciales verificables.
f) Pruebas de conocimiento cero.
g) Historial reputacional voluntario.
h) Auditorías selectivas de wallets.
i) Declaraciones de no contaminación.
j) Pruebas de control de wallet.

Artículo 257. Separación entre Privacidad y Opacidad Ilícita

La privacidad financiera, el pseudonimato, el uso de wallets no custodiales, tecnologías de cifrado o mecanismos de protección transaccional no constituirán presunción de ilicitud.

No obstante, la privacidad no ampara la utilización deliberada de activos digitales para ocultar delitos, lavar fondos, financiar actividades ilícitas, evadir sanciones aplicables, defraudar contrapartes o contaminar mercados regulados.

Artículo 258. Autorregulación del Usuario Self-Custody

Los usuarios de autocustodia que pretendan interactuar con mercados regulados, bolsas de activos digitales, tokenización institucional, bancos blockchain-native, emisores de RWA, plataformas autorizadas, stablecoin

banking o infraestructura pública digital podrán adoptar estándares de autorregulación proporcionados a su nivel de actividad.

La autorregulación podrá consistir en:

a) Separación de wallets por finalidad.
b) Evitar exposición a direcciones sancionadas.
c) Uso de herramientas de análisis de riesgo.
d) Conservación privada de registros de origen de fondos.
e) Uso de credenciales verificables.
f) Declaraciones voluntarias de fuente lícita.
g) Pruebas criptográficas de no exposición.
h) Auditorías selectivas cuando sea necesario.
i) Políticas personales de seguridad de llaves.
j) Gestión de riesgos de contraparte.

SECCIÓN II — COMPLIANCE COMPATIBLE CON PRIVACIDAD

Artículo 259. Compliance Criptográfico

Se reconoce el compliance criptográfico como el conjunto de herramientas, estándares, pruebas, credenciales y procedimientos tecnológicos destinados a demostrar cumplimiento, integridad transaccional, origen razonable de fondos, no exposición a riesgos prohibidos o elegibilidad regulatoria sin revelar información personal o financiera innecesaria.

El compliance criptográfico podrá utilizar:

a) Zero Knowledge Proofs.
b) Credenciales verificables.
c) Identificadores descentralizados.
d) Proof of clean funds.
e) Proof of non-sanction exposure.
f) Proof of wallet control.
g) Proof of reserves.
h) Proof of liabilities.
i) Attestations independientes.
j) Selective disclosure.
k) On-chain risk attestations.
l) Privacy-preserving analytics.

Artículo 260. Zero Knowledge Compliance

La IID promoverá el uso de pruebas de conocimiento cero y mecanismos equivalentes para permitir que usuarios, wallets, entidades y protocolos demuestren condiciones regulatorias específicas sin revelar datos completos.

Podrán acreditarse mediante ZKP, entre otros:

a) No pertenencia a listas de sanciones.
b) Mayoría de edad.
c) Residencia o jurisdicción permitida.
d) Control legítimo de wallet.
e) Cumplimiento de límites transaccionales.
f) No exposición relevante a direcciones ilícitas.
g) Verificación previa por entidad autorizada.

h) Elegibilidad para participar en mercados regulados.
i) Solvencia mínima sin revelar patrimonio total.
j) Cumplimiento de reglas de tokenización o inversión.

Artículo 261. Proof of Clean Funds

La IID podrá reconocer estándares técnicos de proof of clean funds o pruebas equivalentes para acreditar que determinados activos digitales no presentan exposición relevante, directa o indirecta, a actividades ilícitas conocidas, direcciones sancionadas, hacks, ransomware, terrorismo, explotación de personas, fraude significativo o fuentes prohibidas.

Estas pruebas deberán ser proporcionales, verificables, actualizables y no discriminatorias.

El proof of clean funds no deberá convertirse en requisito universal para toda transacción peer-to-peer, sino en herramienta de acceso a mercados regulados, productos institucionales, tokenización, banca digital, liquidez profesional o relaciones comerciales de mayor riesgo.

Artículo 262. Proof of Non-Sanction Exposure

Los usuarios, wallets, plataformas, protocolos o entidades podrán demostrar, mediante mecanismos criptográficos o certificaciones independientes, que no mantienen exposición relevante a direcciones, entidades o personas sujetas a sanciones aplicables.

La verificación de no exposición a sanciones deberá respetar:

a) Minimización de datos.
b) Debido proceso.
c) Posibilidad de revisión.
d) Actualización de listas.
e) Prevención de falsos positivos.
f) Protección contra exclusión arbitraria.
g) No discriminación tecnológica.
h) Privacidad financiera razonable.

Artículo 263. Credenciales Verificables de Compliance

Podrán emitirse credenciales verificables de compliance por entidades autorizadas, auditores independientes, proveedores técnicos reconocidos, VASP, bancos digitales, DAOs certificadas o mecanismos descentralizados aprobados por la IID.

Estas credenciales podrán acreditar:

a) Verificación de identidad previa.
b) Control de wallet.
c) Evaluación de riesgo.
d) Cumplimiento de límites.
e) Origen razonable de fondos.
f) No exposición a sanciones.
g) Perfil de inversionista.
h) Elegibilidad para mercados.
i) Auditoría de actividad específica.
j) Cumplimiento de reglas de tokenización.

El titular de la credencial conservará control sobre cuándo, cómo y ante quién presentarla, salvo requerimiento legal individualizado.

SECCIÓN III — GOVERNANCE DE MERCADOS Y LIQUIDEZ LIMPIA

Artículo 264. Integridad de Liquidez Digital

Los mercados regulados, bolsas de activos digitales, bancos digitales, emisores de RWA, plataformas de tokenización y protocolos institucionales deberán adoptar políticas de integridad de liquidez para prevenir contaminación material de fondos, abuso de mercado, manipulación, fraude, hack proceeds, sanciones y riesgo reputacional sistémico.

Dichas políticas deberán ser proporcionales, transparentes, no discriminatorias y compatibles con autocustodia, privacidad financiera y tecnologías de cumplimiento criptográfico.

Artículo 265. Prevención de Contaminación Sistémica

La IID podrá establecer estándares de prevención de contaminación sistémica en mercados digitales para evitar que activos provenientes de actividades ilícitas afecten pools de liquidez, mercados secundarios, RWA, stablecoins, bancos digitales o plataformas institucionales.

Estos estándares podrán incluir:

a) Segmentación de riesgos.
b) Alertas de exposición.
c) Análisis de rutas transaccionales.
d) Certificaciones voluntarias.
e) Thresholds de riesgo.
f) Freezing policy solo cuando exista base legal.
g) Procedimientos de revisión.
h) Mecanismos de apelación.
i) Uso de ZKP y selective disclosure.
j) Reporte a autoridades cuando corresponda.

Artículo 266. Risk Scoring No Intrusivo

Los sistemas de evaluación de riesgo sobre wallets, transacciones o activos digitales deberán diseñarse de forma no intrusiva, proporcional, auditable, explicable y sujeta a revisión.

El risk scoring no podrá utilizarse para crear scoring social financiero, bloquear arbitrariamente usuarios, discriminar por uso de autocustodia, penalizar privacidad legítima, excluir sin revisión humana, imponer listas negras opacas, sustituir análisis contextual o generar debanking automático.

Todo sistema de risk scoring deberá contar con mecanismos para corregir falsos positivos y permitir explicación razonable del riesgo atribuido. El uso de analítica on-chain no habilitará por sí mismo a la IID ni a sujetos privados a acceder a comunicaciones, documentos privados o datos protegidos fuera de los supuestos autorizados por la Constitución y la ley.

Artículo 267. Reputación Criptográfica Voluntaria

Se reconoce la reputación criptográfica voluntaria como mecanismo mediante el cual una wallet, usuario, DAO, protocolo o entidad puede acreditar historial de integridad, cumplimiento, solvencia, no exposición a riesgos prohibidos o comportamiento confiable sin revelar información innecesaria.

La reputación criptográfica voluntaria no podrá convertirse en sistema obligatorio de scoring social, identidad universal, vigilancia financiera o exclusión automática.

La falta de reputación voluntaria no será presunción de ilicitud, aunque los mercados regulados podrán exigirla de manera proporcional para actividades de mayor riesgo.

SECCIÓN IV — AUTORREGULACIÓN DE PROTOCOLOS, DAOS Y COMUNIDADES

Artículo 268. Códigos de Conducta Web3

Los protocolos, DAOs, comunidades, mercados y proyectos Web3 podrán adoptar códigos de conducta, estándares de integridad, políticas de transparencia, auditoría, gestión de tesorería, ciberseguridad, control de conflictos, disclosure y prevención de abuso.

La IID podrá reconocer estándares de autorregulación cuando sean públicos, verificables, no discriminatorios y compatibles con derechos fundamentales.

Artículo 269. Governance Responsable de DAOs

Las DAOs que administren tesorerías, protocolos, mercados, RWA, liquidez institucional o activos de terceros deberán adoptar mecanismos proporcionales de governance responsable.

Estos podrán incluir:

a) Transparencia de tesorería.
b) Publicación de propuestas.
c) Quórums claros.
d) Control de conflictos.
e) Auditoría de smart contracts.
f) Multisig o mecanismos equivalentes.
g) Reportes de gastos.
h) Límites a insiders.
i) Disclosure de riesgos.
j) Mecanismos de emergencia.
k) Protección de minorías.
l) Gestión de llaves.

Artículo 270. Estándares de Seguridad para Protocolos

Los protocolos que pretendan integrarse con mercados regulados, RWA, stablecoins, bancos digitales o infraestructura institucional deberán adoptar estándares mínimos de seguridad.

Podrán exigirse, según riesgo:

a) Auditoría de smart contracts.
b) Bug bounty.
c) Pruebas formales cuando aplique.
d) Gestión de admin keys.
e) Timelocks.
f) Multisig transparente.
g) Planes de emergencia.
h) Disclosure de riesgos.
i) Auditoría de oráculos.
j) Protección frente a exploits.
k) Simulaciones de estrés.
l) Documentación técnica.

SECCIÓN V — LÍMITES AL COMPLIANCE Y PROTECCIÓN DE DERECHOS

Artículo 271. Prohibición de Vigilancia Financiera Masiva

Ninguna política de compliance, AML/CFT, integridad de mercado, proof of clean funds, risk scoring, reputación criptográfica o autorregulación podrá utilizarse para implementar vigilancia financiera masiva, monitoreo indiscriminado, identificación universal obligatoria, rastreo permanente de wallets o perfilamiento total de personas.

Artículo 272. Prohibición de Whitelisting Estatal Obligatorio

Queda prohibido imponer un sistema estatal general de whitelisting obligatorio de wallets como condición universal para participar en la economía digital, utilizar activos digitales, transferir valor, interactuar peer-to-peer o ejercer autocustodia.

Los mercados regulados podrán adoptar listas de acceso o requisitos de elegibilidad proporcionales para actividades específicas de mayor riesgo, siempre que respeten debido proceso, revisión, privacidad y no discriminación.

Artículo 273. Prohibición de Criminalización de Wallets No Custodiales

El uso, desarrollo, tenencia, descarga, auditoría, promoción o interacción con wallets no custodiales no será criminalizado por sí mismo.

No podrá presumirse ilicitud por:

a) Usar autocustodia.
b) Usar pseudónimos.
c) Utilizar privacidad legítima.
d) Interactuar con protocolos descentralizados.
e) Mantener fondos fuera de custodios regulados.
f) Usar hardware wallets.
g) Operar multisig.
h) Ejecutar smart contracts lícitos.

Artículo 274. Debido Proceso en Bloqueos, Alertas y Exclusiones

Toda decisión de bloquear, congelar, rechazar, excluir, marcar como riesgosa o limitar una wallet, usuario, protocolo o transacción en mercados regulados deberá contar con base objetiva, trazabilidad, motivación suficiente y mecanismo de revisión.

Cuando sea legalmente posible, el usuario deberá tener derecho a:

a) Conocer la razón general de la medida.
b) Aportar prueba de origen de fondos.
c) Corregir falsos positivos.
d) Presentar credenciales o pruebas criptográficas.
e) Solicitar revisión humana.
f) Obtener respuesta razonada.
g) Impugnar conforme a ley.

Artículo 275. Minimización de Datos en Compliance

Los procesos de compliance deberán recolectar, procesar y conservar únicamente la información estrictamente necesaria para la finalidad legítima correspondiente.

Deberán preferirse mecanismos criptográficos, pruebas selectivas, ZKP, credenciales verificables, agregación de riesgo y documentación mínima sobre esquemas de vigilancia o extracción masiva de datos.

SECCIÓN VI — ESTÁNDARES, CERTIFICACIÓN Y COORDINACIÓN INSTITUCIONAL

Artículo 276. Estándares de Compliance Criptográfico

La IID podrá emitir estándares técnicos de compliance criptográfico aplicables a mercados regulados, VASP, bancos digitales, tokenización institucional, RWA, stablecoins y protocolos integrados a infraestructura nacional.

Dichos estándares deberán ser:

a) Proporcionales.
b) Tecnológicamente neutrales.
c) Auditables.
d) Compatibles con privacidad.
e) Interoperables.
f) Revisables periódicamente.
g) Basados en riesgo.
h) No discriminatorios.
i) Compatibles con GAFI/FATF.
j) Respetuosos de autocustodia.

Artículo 277. Certificación de Herramientas de Compliance

La IID podrá reconocer o certificar herramientas de análisis, ZKP compliance, proof of clean funds, wallet reputation, proof of reserves, credenciales verificables, análisis de riesgo y auditoría on-chain, siempre que respeten derechos fundamentales.

La certificación no deberá crear monopolios de proveedores ni obligar al uso de una única herramienta.

Artículo 278. Cooperación con Autoridades AML/CFT

La IID coordinará con autoridades competentes en materia AML/CFT, fiscal, judicial, policial y financiera para prevenir delitos, proteger mercados y cumplir estándares internacionales, sin debilitar autocustodia, privacidad financiera, derechos digitales o infraestructura descentralizada.

Toda cooperación deberá respetar legalidad, finalidad específica, proporcionalidad, debido proceso, protección de datos y prohibición de vigilancia masiva.

Artículo 279. Educación en Autocustodia Responsable

El Estado, la IID, universidades, sector privado y comunidades Web3 promoverán educación sobre autocustodia responsable, seguridad de llaves, prevención de fraudes, higiene transaccional, privacidad, análisis de riesgo, compliance criptográfico y protección de usuarios.

La educación deberá empoderar, no asustar; prevenir abusos, no desalentar innovación.

SECCIÓN VII — CLÁUSULA FINAL DE SOBERANÍA FINANCIERA RESPONSABLE

Artículo 280. Cláusula de Equilibrio entre Libertad y Legitimidad

Toda norma, política, estándar, certificación o práctica relacionada con autocustodia, compliance, AML/CFT, wallet risk, proof of clean funds, governance digital o acceso a mercados deberá interpretarse conforme al equilibrio entre libertad financiera y legitimidad institucional.

Será contrario a este marco todo diseño que:

a) Criminalice autocustodia.
b) Imponga vigilancia masiva.

c) Convierta wallets en permisos estatales.
d) Elimine privacidad financiera.
e) Facilite contaminación sistémica.
f) Permita fondos ilícitos en mercados regulados.
g) Excluya sin debido proceso.
h) Genere listas negras opacas.
i) Capture compliance en monopolios privados.
j) Haga imposible interactuar lícitamente con mercados institucionales desde autocustodia.

CAPÍTULO X — INTELIGENCIA ARTIFICIAL, AUTOMATIZACIÓN Y SOBERANÍA ALGORÍTMICA

SECCIÓN I — PRINCIPIOS GARANTISTAS DE INTELIGENCIA ARTIFICIAL

Artículo 281. Inteligencia Artificial Compatible con Derechos Fundamentales

La inteligencia artificial utilizada por el Estado o por sujetos regulados dentro del ámbito de esta ley deberá ser compatible con dignidad humana, igualdad, privacidad, debido proceso, no discriminación, seguridad, transparencia y control humano proporcional al riesgo.

La rectoría general de política pública en inteligencia artificial corresponderá al MICITT y las competencias de protección de datos, consumo, competencia, salud, educación, seguridad, justicia u otras materias permanecerán en las autoridades legalmente competentes.

La IID ejercerá atribuciones sobre inteligencia artificial únicamente cuando se utilice en mercados digitales, servicios o sujetos bajo su supervisión, en infraestructura digital crítica comprendida por esta ley o en auditorías técnicas expresamente encomendadas, sin convertirse en regulador general de toda aplicación de inteligencia artificial en Costa Rica.

Artículo 282. Soberanía Algorítmica

Costa Rica reconoce la soberanía algorítmica como la capacidad del Estado, las personas, las comunidades, la academia y el sector productivo de comprender, auditar, desarrollar, modificar, supervisar, interoperar y controlar los sistemas automatizados que afectan derechos, economía, infraestructura pública y democracia.

La soberanía algorítmica implica evitar dependencia absoluta de modelos cerrados, proveedores únicos, sistemas opacos, plataformas extranjeras no auditables o infraestructura tecnológica que impida control democrático.

Artículo 283. Transparencia Algorítmica

Todo sistema algorítmico utilizado por instituciones públicas o por entidades privadas en servicios de relevancia pública deberá ser transparente en la medida necesaria para permitir control, auditoría, explicación, impugnación y rendición de cuentas.

La transparencia algorítmica podrá comprender:

a) Finalidad del sistema.
b) Autoridad o entidad responsable.
c) Tipo de datos utilizados.
d) Criterios generales de decisión.
e) Riesgos conocidos.
f) Medidas de mitigación.
g) Auditorías realizadas.
h) Mecanismos de revisión humana.

i) Procedimientos de reclamación.
j) Impacto sobre derechos fundamentales.

Artículo 284. Primacía Humana

La inteligencia artificial no podrá sustituir la responsabilidad humana en decisiones que afecten derechos fundamentales, libertad, propiedad, identidad, acceso financiero, salud, educación, justicia, empleo, participación política o servicios públicos esenciales.

Toda decisión automatizada de alto impacto deberá contar con supervisión humana significativa, responsabilidad institucional identificable y posibilidad real de revisión.

SECCIÓN II — DERECHOS FRENTE A SISTEMAS AUTOMATIZADOS

Artículo 285. Derecho a Explicación Algorítmica

Toda persona afectada por una decisión automatizada o asistida por inteligencia artificial tendrá derecho a recibir una explicación clara, comprensible y suficiente sobre la lógica general, criterios principales, datos relevantes y efectos de dicha decisión.

Este derecho será especialmente exigible cuando la decisión afecte:

a) Acceso financiero.
b) Crédito.
c) Identidad digital.
d) Servicios públicos.
e) Salud.
f) Educación.
g) Empleo.
h) Justicia.
i) Seguridad.
j) Migración.
k) Beneficios sociales.
l) Propiedad digital.
m) Participación electoral.
n) Perfil reputacional.

Artículo 286. Derecho a Revisión Humana

Toda persona tendrá derecho a solicitar revisión humana efectiva de decisiones automatizadas que produzcan efectos jurídicos, económicos, patrimoniales, reputacionales, financieros, laborales, educativos, sanitarios, electorales o administrativos relevantes.

La revisión humana deberá ser real, competente, documentada y capaz de modificar, revocar o corregir la decisión automatizada.

Artículo 287. Prohibición de Decisiones Totalmente Automatizadas en Derechos Fundamentales

Queda prohibido que decisiones que afecten sustancialmente derechos fundamentales sean adoptadas exclusivamente por sistemas automatizados sin intervención humana significativa.

Esta prohibición aplica especialmente a:

a) Restricción de libertad.
b) Bloqueo financiero.
c) Exclusión de servicios esenciales.

d) Determinaciones electorales.
e) Decisiones judiciales.
f) Sanciones administrativas graves.
g) Acceso a salud.
h) Acceso a educación.
i) Cancelación de identidad digital.
j) Bloqueo de wallets o activos digitales.
k) Clasificación de riesgo con efecto excluyente.

Artículo 288. Derecho a Impugnación y Reparación Algorítmica

Toda persona afectada por error, sesgo, discriminación, exclusión, daño patrimonial, bloqueo, pérdida de oportunidad o afectación de derechos causada por inteligencia artificial o sistemas automatizados tendrá derecho a impugnar, corregir y solicitar reparación.

El responsable del sistema deberá conservar trazabilidad suficiente para investigar la decisión, identificar causas y corregir efectos.

SECCIÓN III — LÍMITES LEGALES A LA IA ESTATAL

Artículo 289. Prohibición de IA para Vigilancia Masiva

Queda prohibido el uso de inteligencia artificial para vigilancia masiva, monitoreo indiscriminado, reconocimiento generalizado de personas, rastreo permanente, análisis conductual poblacional, identificación biométrica indiscriminada o vigilancia financiera generalizada.

La IA estatal solo podrá utilizarse para fines específicos, proporcionales, legalmente autorizados, auditables, temporales y sujetos a control independiente.

Artículo 290. Prohibición de Scoring Social Algorítmico

Queda prohibido crear o utilizar sistemas de inteligencia artificial destinados a asignar puntajes sociales, reputacionales, políticos, ideológicos, conductuales o morales que condicionen derechos, servicios públicos, acceso financiero, movilidad, educación, salud, empleo, crédito, propiedad o participación digital.

Artículo 291. Prohibición de Perfilamiento Político Automatizado

Queda prohibido utilizar IA estatal o sistemas automatizados para inferir, clasificar, monitorear o predecir afiliación política, ideología, voto, disidencia, participación cívica, activismo, opinión pública individual o conducta electoral de las personas.

Artículo 292. Prohibición de IA Electoral Manipulativa

Queda prohibido el uso de IA para manipular procesos electorales, producir desinformación política automatizada, generar deepfakes electorales engañosos, microsegmentar propaganda opaca, suplantar candidatos, alterar percepción pública mediante bots coordinados o interferir ilícitamente en la formación libre de la voluntad popular.

Artículo 293. Prohibición de Censura Algorítmica Estatal

El Estado no podrá utilizar IA para censurar, degradar, ocultar, despriorizar o bloquear expresiones lícitas, opiniones políticas, investigación periodística, crítica pública, actividad cívica o participación digital sin base legal expresa, debido proceso y control independiente.

SECCIÓN IV — IA, IDENTIDAD, BIOMETRÍA Y PRIVACIDAD FINANCIERA

Artículo 294. IA y Protección Biométrica

Todo sistema de IA que procese datos biométricos deberá someterse a estándares reforzados de legalidad, necesidad, proporcionalidad, seguridad, auditoría, minimización, finalidad específica, retención limitada y revisión independiente.

Queda prohibido el uso de biometría algorítmica para vigilancia generalizada, scoring social, persecución política, control financiero o identificación indiscriminada.

Artículo 295. Restricciones al Reconocimiento Facial

El reconocimiento facial en espacios públicos o servicios esenciales solo podrá utilizarse de forma excepcional, mediante ley expresa, finalidad legítima, proporcionalidad estricta, supervisión independiente y garantías contra abuso.

Queda prohibido el reconocimiento facial masivo, permanente o preventivo de población no investigada.

Artículo 296. IA y Privacidad Financiera

Queda prohibido utilizar IA para vigilancia financiera masiva, perfilamiento económico indiscriminado, censura financiera automatizada, bloqueo algorítmico de activos, exclusión bancaria sin revisión humana o clasificación de wallets sin debido proceso.

Los sistemas de análisis financiero basados en IA deberán ser proporcionales, auditables, explicables, sujetos a revisión humana y compatibles con autocustodia, privacidad financiera y compliance criptográfico.

Artículo 297. IA, Identidad Digital y Wallets

Los sistemas de IA no podrán utilizar identidad digital, wallets, credenciales, transacciones, biometría o actividad on-chain para construir perfiles integrales de conducta sin consentimiento válido, base legal expresa y finalidad legítima.

Queda prohibida la fusión automatizada de identidad, finanzas, comportamiento, política y biometría para control social.

SECCIÓN V — TRANSPARENCIA, AUDITORÍA Y REGISTRO DE IA

Artículo 298. Auditoría de Sistemas de IA

Todo sistema de IA de alto impacto utilizado por el Estado o por entidades privadas en servicios esenciales deberá someterse a auditoría técnica, jurídica, ética, de seguridad y de derechos fundamentales.

La auditoría deberá evaluar:

a) Sesgos.
b) Exactitud.
c) Seguridad.
d) Calidad de datos.
e) Explicabilidad.
f) Riesgos de discriminación.
g) Impacto en derechos.
h) Riesgos de vigilancia.
i) Gobernanza.
j) Ciberseguridad.

k) Dependencia tecnológica.
l) Mecanismos de reparación.

Artículo 299. Registro Público de IA Estatal Crítica

El Estado deberá mantener un registro público de sistemas de IA críticos utilizados por instituciones públicas, salvo excepciones estrictamente justificadas por seguridad legítima.

El registro incluirá:

a) Institución responsable.
b) Finalidad.
c) Proveedor.
d) Tipo de sistema.
e) Datos utilizados.
f) Impacto esperado.
g) Evaluaciones realizadas.
h) Medidas de mitigación.
i) Responsable humano.
j) Mecanismo de reclamo.

Artículo 300. Evaluación de Impacto Algorítmico

Antes de implementar IA de alto impacto, toda institución pública deberá realizar evaluación de impacto algorítmico que determine riesgos para derechos fundamentales, privacidad, no discriminación, seguridad, libertad financiera, identidad digital, democracia y dignidad humana.

La evaluación deberá publicarse salvo reserva excepcional motivada.

Artículo 301. Trazabilidad y Bitácora Algorítmica

Los sistemas de IA de alto impacto deberán conservar registros suficientes de funcionamiento, entradas relevantes, salidas, versiones, cambios, auditorías, responsables y decisiones tomadas, para permitir investigación, impugnación y rendición de cuentas.

SECCIÓN VI — INNOVACIÓN, IA ABIERTA Y DESCENTRALIZADA

Artículo 302. Protección de IA Open Source

El desarrollo, publicación, auditoría, investigación, entrenamiento, documentación, distribución o uso de modelos de IA open source no constituirá por sí mismo actividad ilícita ni regulada de alto riesgo.

La responsabilidad surgirá cuando exista uso dañino, negligencia grave, incumplimiento legal, manipulación deliberada, fraude, vigilancia ilícita o afectación concreta de derechos.

Artículo 303. IA Descentralizada

El Estado promoverá la investigación y desarrollo de inteligencia artificial descentralizada, federada, verificable, auditable, interoperable, privada por diseño y compatible con infraestructura blockchain.

La IA descentralizada podrá utilizarse para:

a) Preservar privacidad.
b) Reducir dependencia de proveedores únicos.
c) Distribuir capacidades computacionales.
d) Facilitar auditoría.

e) Mejorar transparencia.
f) Proteger datos locales.
g) Fortalecer soberanía tecnológica.

Artículo 304. Sandboxes de IA y Blockchain

La IID, junto con autoridades competentes, podrá promover sandboxes de IA, blockchain, identidad soberana, compliance criptográfico, tokenización, DeFi, ciberseguridad y automatización pública.

Los sandboxes deberán respetar derechos fundamentales, consentimiento informado, ciberseguridad, no discriminación, privacidad y supervisión proporcional.

Artículo 305. Desarrollo Nacional de Talento Algorítmico

El Estado promoverá formación nacional en inteligencia artificial, auditoría algorítmica, criptografía, blockchain, ciberseguridad, ética tecnológica, privacidad, análisis de datos y regulación digital.

SECCIÓN VII — DEEPFAKES, MANIPULACIÓN Y AUTENTICIDAD DIGITAL

Artículo 306. Identificación de Contenido Sintético de Alto Impacto

La ley podrá exigir identificación, marcas de procedencia, trazabilidad o divulgación de contenido sintético generado por IA cuando pueda afectar procesos electorales, reputación, mercados financieros, seguridad pública, menores de edad, identidad personal o derechos fundamentales.

Las obligaciones deberán ser proporcionales y no podrán utilizarse para censurar expresión legítima, sátira, arte, investigación o crítica política.

Artículo 307. Protección frente a Deepfakes Dañinos

Queda prohibido utilizar IA para suplantar identidad, fabricar evidencia falsa, manipular mercados, afectar procesos electorales, extorsionar, defraudar, dañar reputación, vulnerar intimidad o inducir a error grave mediante contenido sintético engañoso.

Artículo 308. Derecho a Autenticidad Digital

Toda persona tiene derecho a mecanismos razonables para demostrar autenticidad, origen, integridad y no manipulación de documentos, imágenes, audio, video, credenciales, identidad y comunicaciones digitales.

El Estado promoverá herramientas criptográficas, firmas digitales, blockchain, hashes, credenciales verificables y sellos de tiempo para fortalecer autenticidad digital.

SECCIÓN VIII — CLÁUSULAS FINALES DE GARANTÍA Y CONTROL

Artículo 309. Cláusula de Dignidad Humana frente a IA

Toda inteligencia artificial utilizada en Costa Rica deberá interpretarse y aplicarse conforme a la dignidad humana, autonomía individual, libertad, privacidad, igualdad, pluralismo, no discriminación, debido proceso, libertad financiera, identidad soberana y protección frente a vigilancia masiva.

Artículo 310. Cláusula de Primacía Humana

Ningún sistema de IA podrá tener autoridad final e irrevisable sobre derechos fundamentales, sanciones, libertades, propiedad, identidad, patrimonio, acceso económico, participación política o vida democrática.

Siempre deberá existir una persona o institución responsable.

Artículo 311. Cláusula Anti-Distopía Digital

Será contrario al orden constitucional todo sistema de inteligencia artificial, automatización o analítica de datos que, directa o indirectamente, tenga por finalidad o efecto:

a) Vigilancia masiva.
b) Scoring social.
c) Censura algorítmica.
d) Control financiero automatizado.
e) Perfilamiento político.
f) Identificación biométrica indiscriminada.
g) Manipulación electoral.
h) Fusión total de identidad, dinero y conducta.
i) Exclusión automatizada sin debido proceso.
j) Sustitución de ciudadanía libre por administración algorítmica de la vida.

CAPÍTULO XI — CIBERSEGURIDAD NACIONAL, RESILIENCIA DIGITAL Y SOBERANÍA TECNOLÓGICA

SECCIÓN I — PRINCIPIOS DE SOBERANÍA TECNOLÓGICA

Artículo 312. Soberanía Tecnológica Nacional

Costa Rica reconoce la soberanía tecnológica como la capacidad del Estado, las personas, las empresas, la academia y la sociedad civil de desarrollar, auditar, operar, proteger, migrar e interoperar infraestructura digital crítica sin dependencia irreversible de proveedores, plataformas, gobiernos extranjeros, nubes opacas, sistemas cerrados o tecnologías no auditables.

La soberanía tecnológica no implica aislamiento, sino capacidad real de decisión, auditoría, resiliencia y control democrático sobre la infraestructura que sostiene derechos fundamentales, economía digital, identidad, elecciones, registros públicos, mercados financieros y servicios esenciales.

Artículo 313. Infraestructura Digital Estratégica

Será considerada infraestructura digital estratégica toda aquella que soporte o afecte:

a) Identidad digital soberana.
b) Registro Público blockchain.
c) Sistema electoral digital.
d) Mercados de activos digitales.
e) Bolsa de Activos Digitales.
f) Banca digital soberana.
g) Stablecoins y liquidación on-chain.
h) Sistemas públicos de IA.
i) Ciberseguridad nacional.
j) Salud, educación, justicia y servicios esenciales.
k) Telecomunicaciones.
l) Datos públicos críticos.
m) Infraestructura cloud estatal.
n) Sistemas de pagos.
o) Llaves criptográficas estatales.
p) Smart contracts estatales.

Artículo 314. Independencia Tecnológica Crítica

El Estado no podrá diseñar, contratar o mantener infraestructura estratégica bajo condiciones de dependencia irreversible, opacidad técnica, imposibilidad de auditoría, ausencia de portabilidad, bloqueo contractual, falta de transferencia de conocimiento o control exclusivo de un proveedor.

Todo contrato o sistema crítico deberá prever:

a) Portabilidad.
b) Reversibilidad.
c) Auditoría independiente.
d) Interoperabilidad.
e) Continuidad operativa.
f) Documentación técnica.
g) Acceso a registros.
h) Gestión soberana de llaves.
i) Plan de migración.
j) Evaluación de riesgo de proveedor.

SECCIÓN II — INFRAESTRUCTURA CRÍTICA DIGITAL

Artículo 315. Protección de Infraestructura Blockchain Estatal

Toda infraestructura blockchain utilizada por el Estado deberá cumplir estándares reforzados de seguridad, resiliencia, gestión de llaves, auditoría de smart contracts, monitoreo de integridad, continuidad operativa, protección de datos, interoperabilidad y prevención de captura tecnológica.

Los sistemas blockchain públicos deberán diseñarse con:

a) Redundancia.
b) Nodos distribuidos.
c) Gobernanza clara.
d) Logs verificables.
e) Auditoría externa.
f) Minimización de datos personales.
g) Planes de emergencia.
h) Actualización segura.
i) Protección contra ataques de consenso.
j) Evaluación de riesgo post-cuántico.

Artículo 316. Protección de Sistemas Electorales Digitales

Los sistemas electorales digitales serán infraestructura crítica de máxima protección constitucional.

Deberán contar con auditoría técnica independiente, pruebas de penetración, trazabilidad, control de proveedores, gestión segura de llaves, software verificable, protección contra deepfakes, protección contra manipulación algorítmica, continuidad operativa, respaldo físico cuando corresponda y mecanismos de recuperación ante incidentes.

Artículo 317. Protección del Registro Público Blockchain

El Registro Público blockchain y sus sistemas interoperables deberán contar con mecanismos de integridad, disponibilidad, ciberseguridad, recuperación ante desastres, auditoría, gestión de llaves, trazabilidad de modificaciones, protección de datos y defensa contra alteración maliciosa.

Toda actualización, migración o corrección deberá preservar historial verificable.

Artículo 318. Protección de Identidad Digital Soberana

La infraestructura de identidad digital soberana deberá proteger credenciales, identificadores, llaves, biometría, atributos verificables y mecanismos de autenticación contra robo, suplantación, vigilancia, correlación indebida, ataques cuánticos futuros, pérdida irreversible o captura por proveedor único.

Se deberán aplicar estándares de privacidad por diseño, minimización, recuperación segura, revocación, portabilidad e interoperabilidad.

Artículo 319. Protección de Infraestructura Financiera Web3

La Bolsa de Activos Digitales, bancos blockchain-native, custodios, sistemas de pago, stablecoin banking, DeFi institucional, mercados secundarios, smart contracts financieros y sistemas de liquidación on-chain deberán cumplir estándares reforzados de ciberseguridad, gestión de riesgos, proof of reserves, segregación de activos, auditoría, resiliencia y protección de usuarios.

SECCIÓN III — CRIPTOGRAFÍA, POST-QUANTUM SECURITY Y SEGURIDAD NACIONAL

Artículo 320. Protección Reforzada de la Criptografía

La criptografía será reconocida como infraestructura esencial de seguridad nacional, privacidad, libertad financiera, identidad soberana, autenticidad documental, protección de datos, ciberseguridad y confianza digital.

El Estado deberá promover el uso de criptografía fuerte en sistemas públicos y privados de relevancia crítica.

Artículo 321. Prohibición de Backdoors Obligatorias

Queda prohibido exigir puertas traseras, debilitamiento deliberado del cifrado, acceso secreto, vulnerabilidades obligatorias, escaneo indiscriminado o mecanismos universales de intervención en sistemas criptográficos, wallets, comunicaciones, identidad digital, smart contracts, dispositivos o infraestructura digital.

Las investigaciones legítimas deberán realizarse mediante medidas individualizadas, autorizadas por ley, proporcionales y sujetas a debido proceso.

Artículo 322. Gestión Segura de Llaves Criptográficas

Toda institución pública o entidad regulada que administre llaves criptográficas críticas deberá implementar políticas de generación, custodia, rotación, recuperación, destrucción, auditoría y control de acceso.

La gestión de llaves deberá evitar concentración unipersonal, uso no autorizado, pérdida irreversible, dependencia de terceros, exposición innecesaria y ausencia de trazabilidad.

Podrán utilizarse esquemas de multifirma, hardware security modules, threshold signatures, separación de funciones, bitácoras verificables, controles de emergencia y auditoría periódica.

Artículo 323. Estrategia Nacional de Criptografía Post-Cuántica

Costa Rica deberá adoptar una Estrategia Nacional de Criptografía Post-Cuántica para preparar infraestructura crítica frente al riesgo de computación cuántica capaz de comprometer criptografía asimétrica tradicional.

La estrategia deberá incluir:

a) Inventario criptográfico nacional.
b) Identificación de sistemas vulnerables.
c) Priorización de infraestructura crítica.
d) Plan de migración gradual.

e) Criptoagilidad.
f) Evaluación de estándares internacionales.
g) Pilotos post-cuánticos.
h) Capacitación técnica.
i) Protección contra ataques “harvest now, decrypt later”.
j) Calendarios de transición.
k) Coordinación pública-privada.
l) Actualización periódica.

NIST publicó FIPS 203 para ML-KEM, un mecanismo de encapsulación de claves diseñado para resistir adversarios con computadoras cuánticas; también aprobó estándares para firmas digitales post-cuánticas.

Artículo 324. Criptoagilidad

Toda infraestructura digital estratégica deberá diseñarse con criptoagilidad, entendida como la capacidad de actualizar, reemplazar o combinar algoritmos criptográficos sin interrumpir servicios esenciales ni comprometer integridad histórica.

La criptoagilidad será obligatoria para sistemas de identidad digital, registro público blockchain, banca digital, infraestructura electoral, smart contracts estatales, certificados digitales, comunicaciones oficiales y sistemas de archivo de largo plazo.

Artículo 325. Protección contra Harvest Now, Decrypt Later

El Estado deberá proteger información sensible de largo plazo frente a amenazas de captura actual y descifrado futuro mediante computación cuántica.

Se considerarán especialmente protegidos:

a) Datos biométricos.
b) Información electoral.
c) Expedientes judiciales.
d) Información sanitaria.
e) Datos fiscales.
f) Llaves estatales.
g) Secretos de infraestructura.
h) Identidad digital.
i) Comunicaciones oficiales.
j) Documentos estratégicos.
k) Datos financieros.
l) Registros de seguridad nacional.

SECCIÓN IV — RESILIENCIA Y CIBERDEFENSA DEMOCRÁTICA

Artículo 326. Estrategia Nacional de Ciberresiliencia

El Estado deberá adoptar una Estrategia Nacional de Ciberresiliencia para infraestructura digital crítica, orientada a prevenir, resistir, responder y recuperarse frente a incidentes cibernéticos, fallos sistémicos, sabotaje, ataques de ransomware, manipulación de datos, ataques a smart contracts, ataques de cadena de suministro y amenazas cuánticas.

Artículo 327. Continuidad Operativa Digital

Toda infraestructura digital estratégica deberá contar con planes de continuidad operativa, recuperación ante desastres, respaldo verificable, redundancia, pruebas periódicas, simulacros y mecanismos de restauración segura.

Artículo 328. Respuesta a Incidentes Críticos

Las instituciones públicas y entidades reguladas deberán contar con protocolos de respuesta a incidentes críticos que incluyan:

a) Detección temprana.
b) Contención.
c) Notificación.
d) Preservación de evidencia.
e) Coordinación interinstitucional.
f) Comunicación pública responsable.
g) Recuperación.
h) Análisis post-incidente.
i) Reparación.
j) Actualización de controles.

Artículo 329. Cooperación Público-Privada en Ciberseguridad

El Estado promoverá cooperación con sector privado, universidades, comunidades técnicas, investigadores, operadores de infraestructura, comunidades Web3 y organismos internacionales para fortalecer ciberseguridad nacional.

Dicha cooperación deberá respetar derechos fundamentales, privacidad, transparencia y prohibición de vigilancia masiva.

SECCIÓN V — DEPENDENCIA TECNOLÓGICA, CLOUD SOVEREIGNTY Y SUPPLY CHAIN

Artículo 330. Evaluación de Riesgo Tecnológico Estratégico

Todo proyecto tecnológico público crítico deberá someterse a evaluación de riesgo tecnológico estratégico antes de su contratación o implementación.

La evaluación deberá analizar:

a) Dependencia de proveedor.
b) Jurisdicción del proveedor.
c) Acceso a datos.
d) Riesgos de backdoors.
e) Auditoría posible.
f) Transferencia de conocimiento.
g) Portabilidad.
h) Reversibilidad.
i) Ciberseguridad.
j) Riesgo de sanciones o presión geopolítica.
k) Riesgo de interrupción.
l) Compatibilidad post-cuántica.

Artículo 331. Seguridad de Proveedores Críticos

Los proveedores de infraestructura digital crítica deberán cumplir requisitos de seguridad, transparencia, auditoría, control de subcontratistas, gestión de vulnerabilidades, continuidad operativa, protección de datos, reversibilidad y cooperación ante incidentes.

Artículo 332. Cloud Sovereignty

La infraestructura cloud utilizada para datos, sistemas o servicios críticos deberá cumplir estándares de soberanía, seguridad, auditabilidad, localización o control jurisdiccional cuando corresponda, cifrado fuerte, portabilidad, reversibilidad y continuidad operativa.

El Estado deberá evitar dependencia absoluta de una sola nube, proveedor o jurisdicción.

Artículo 333. Protección de Datos Estratégicos Nacionales

Los datos estratégicos nacionales deberán protegerse contra acceso indebido, transferencia no autorizada, explotación comercial ilegítima, entrenamiento algorítmico no consentido, vigilancia extranjera, ataques de cadena de suministro y descifrado futuro.

SECCIÓN VI — INFRAESTRUCTURA DESCENTRALIZADA Y RESILIENCIA WEB3

Artículo 334. Protección de Nodos y Validadores

La operación lícita de nodos, validadores, infraestructura de consenso, exploradores, oráculos, puentes, indexadores y sistemas descentralizados será protegida como parte de la resiliencia digital nacional.

No podrá restringirse arbitrariamente la operación de infraestructura descentralizada, salvo por razones legítimas, proporcionales y debidamente motivadas.

Artículo 335. Resiliencia de Redes Descentralizadas

El Estado promoverá la diversidad de redes, nodos, validadores, proveedores, geografías, mecanismos de consenso, capas de interoperabilidad y sistemas de respaldo para evitar puntos únicos de falla.

Artículo 336. Interoperabilidad Segura

Toda interoperabilidad entre sistemas estatales, privados y descentralizados deberá diseñarse con controles de seguridad, autenticación fuerte, minimización de datos, trazabilidad, control de permisos, auditoría y protección contra ataques de puente o integración.

Artículo 337. Resiliencia Energética Digital

La infraestructura digital crítica deberá considerar continuidad energética, redundancia eléctrica, eficiencia, integración con energías renovables, protección de centros de datos y planes de contingencia.

SECCIÓN VII — INVESTIGACIÓN, TALENTO Y SECURITY RESEARCH

Artículo 338. Formación Nacional en Ciberseguridad

El Estado promoverá formación técnica y profesional en ciberseguridad, criptografía, blockchain, IA, auditoría de smart contracts, seguridad post-cuántica, análisis forense digital, seguridad cloud e infraestructura crítica.

Artículo 339. Investigación en Seguridad Blockchain, IA y Post-Cuántica

Costa Rica impulsará investigación en seguridad blockchain, inteligencia artificial segura, identidad soberana, criptografía post-cuántica, privacidad, ZKP, ciberdefensa, smart contracts y resiliencia digital.

Artículo 340. Protección de Investigadores de Seguridad

Las personas que realicen investigación de seguridad, auditoría, divulgación responsable de vulnerabilidades, pruebas autorizadas, análisis criptográfico o revisión de infraestructura digital no serán sancionadas por el solo

hecho de identificar vulnerabilidades, siempre que actúen de buena fe, sin explotación abusiva, sin apropiación indebida y conforme a reglas de divulgación responsable.

Artículo 341. Programas de Bug Bounty y Divulgación Responsable

Las instituciones públicas y entidades reguladas podrán implementar programas de bug bounty, canales de reporte, recompensas, protección de investigadores y protocolos de corrección de vulnerabilidades.

SECCIÓN VIII — CLÁUSULAS FINALES DE GARANTÍA

Artículo 342. Cláusula de Resiliencia Democrática Digital

Toda infraestructura digital pública o de relevancia sistémica deberá interpretarse y desarrollarse conforme al principio de resiliencia democrática digital: continuidad de derechos, transparencia, seguridad, auditabilidad, privacidad y capacidad de recuperación frente a ataques, fallos, captura o amenazas futuras.

Artículo 343. Cláusula Anti-Captura Tecnológica

Será contrario al interés público todo diseño tecnológico que concentre control crítico en proveedores opacos, entidades no auditables, monopolios de infraestructura, gobiernos extranjeros, sistemas cerrados, llaves centralizadas o contratos que impidan migración.

Artículo 344. Cláusula de Soberanía Computacional

Costa Rica deberá promover capacidad nacional y regional para acceder, auditar, operar y desarrollar infraestructura computacional crítica, incluyendo cloud, IA, blockchain, criptografía, seguridad post-cuántica, datos estratégicos y redes descentralizadas.

La soberanía computacional será condición esencial para preservar independencia institucional, competitividad económica, seguridad nacional y derechos fundamentales.

CAPÍTULO XII — REGISTRO PÚBLICO BLOCKCHAIN, SMART CONTRACTS ESTATALES, PROPIEDAD PROGRAMABLE Y FE PÚBLICA CRIPTOGRÁFICA

SECCIÓN I — PRINCIPIOS DEL REGISTRO PÚBLICO DIGITAL

Artículo 345. Modernización del Registro Público

El Estado deberá modernizar progresivamente el Registro Público y demás registros oficiales mediante tecnologías blockchain, registros distribuidos, sellos de tiempo, hashes criptográficos, firmas digitales, credenciales verificables, smart contracts y mecanismos de interoperabilidad institucional.

La modernización registral tendrá como finalidad fortalecer seguridad jurídica, trazabilidad, transparencia, eficiencia, prevención de fraude, protección de propiedad, reducción de corrupción, interoperabilidad pública y confianza ciudadana.

La implementación tecnológica no podrá debilitar derechos adquiridos, debido proceso, fe pública, protección de datos, acceso a justicia, control registral ni garantías de terceros.

Artículo 346. Blockchain como Infraestructura Registral

Blockchain y los registros distribuidos serán reconocidos como infraestructura registral complementaria para anclar, verificar, auditar y preservar la integridad de asientos, documentos, certificaciones, anotaciones, modificaciones, gravámenes, cancelaciones, planos, resoluciones y actos registrales relevantes.

El Registro Público blockchain operará bajo un modelo híbrido, donde el sistema registral jurídico conservará su fuerza legal conforme al ordenamiento vigente, y la capa blockchain funcionará como mecanismo de integridad, trazabilidad, evidencia técnica, auditoría pública y prevención de manipulación.

Artículo 347. Principio de Trazabilidad Registral

Todo acto registral relevante deberá contar con trazabilidad suficiente para identificar su origen, fecha, responsable institucional, documento soporte, secuencia, modificación, estado y relación con actos anteriores o posteriores.

La trazabilidad deberá permitir reconstruir el historial registral sin ediciones invisibles, sustituciones opacas, eliminación retroactiva o alteraciones no documentadas.

Las correcciones, rectificaciones, nulidades, cancelaciones o modificaciones deberán quedar técnicamente registradas, preservando el historial verificable del acto original.

Artículo 348. Principio de Interoperabilidad Jurídica

El Registro Público blockchain deberá interoperar con Catastro, municipalidades, notariado digital, autoridades tributarias, autoridades judiciales, sistemas de contratación pública, registros corporativos, registros de garantías, propiedad intelectual, autoridades ambientales y demás instituciones vinculadas a derechos registrables.

La interoperabilidad deberá basarse en estándares abiertos, APIs seguras, minimización de datos, control de acceso, trazabilidad, protección de datos personales, privacidad por diseño y seguridad criptográfica.

SECCIÓN II — REGISTRO PÚBLICO BLOCKCHAIN NACIONAL

Artículo 349. Registro Público Blockchain Nacional

Créase la figura del Registro Público Blockchain Nacional como capa tecnológica de integridad, trazabilidad y verificación aplicable al Registro Nacional y demás registros oficiales que determine la ley.

El Registro Público Blockchain Nacional podrá utilizarse para:

a) Propiedad inmueble.
b) Catastro.
c) Personas jurídicas.
d) Bienes muebles registrables.
e) Garantías mobiliarias.
f) Propiedad intelectual.
g) Gravámenes.
h) Fideicomisos.
i) Poderes.
j) Certificaciones.
k) Documentos notariales verificables.
l) Activos tokenizados.
m) Actos administrativos registrables.
n) Concesiones y permisos.
o) Archivos históricos críticos.

Artículo 350. Integridad e Inmutabilidad Registral

Los actos y documentos anclados en el Registro Público Blockchain Nacional deberán contar con mecanismos de integridad e inmutabilidad técnica que impidan alteraciones silenciosas o no autorizadas.

La inmutabilidad no impedirá rectificaciones legales, nulidades, cancelaciones o modificaciones legítimas. Dichas actuaciones deberán registrarse como nuevos eventos verificables, vinculados al historial original.

Artículo 351. Timestamps, Hashes y Sellos Criptográficos

El Registro Público podrá emitir, registrar o reconocer sellos criptográficos, hashes, timestamps, firmas digitales, pruebas de existencia, certificados verificables y demás mecanismos técnicos que acrediten fecha, integridad, autenticidad y secuencia de documentos o actos.

Estos mecanismos podrán utilizarse para:

a) Escrituras públicas.
b) Certificaciones registrales.
c) Planos catastrales.
d) Asientos registrales.
e) Poderes.
f) Contratos privados.
g) Documentos societarios.
h) Documentos administrativos.
i) Evidencia judicial.
j) Smart contracts.
k) Activos tokenizados.

Artículo 352. Archivo Histórico Verificable

El Estado deberá preservar archivos registrales, notariales, administrativos y documentales críticos mediante mecanismos digitales verificables que permitan comprobar integridad histórica, autenticidad, secuencia y no alteración.

El archivo histórico verificable deberá protegerse contra pérdida, manipulación, corrupción de datos, ataques cibernéticos, dependencia tecnológica, obsolescencia y amenazas post-cuánticas.

SECCIÓN III — FE PÚBLICA CRIPTOGRÁFICA

Artículo 353. Reconocimiento de la Fe Pública Criptográfica

Se reconoce la fe pública criptográfica como la capacidad jurídica y técnica de acreditar, mediante mecanismos criptográficos verificables, la existencia, integridad, fecha, autenticidad, secuencia, titularidad, consentimiento o ejecución de actos, documentos, registros o transacciones digitales.

La fe pública criptográfica no sustituye la fe pública notarial, judicial, administrativa o registral, salvo disposición legal expresa. La complementa y fortalece mediante evidencia técnica objetiva.

Artículo 354. Alcance de la Fe Pública Criptográfica

La fe pública criptográfica podrá producir efectos probatorios respecto de: a) existencia de un documento en fecha determinada; b) integridad de un archivo; c) control técnico de una llave criptográfica; d) firma digital o criptográfica; e) ejecución de smart contracts; f) secuencia de eventos registrales; g) emisión de credenciales verificables; h) titularidad técnica de activos digitales; i) trazabilidad de actos públicos; j) anclaje de documentos notariales; k) verificación de certificaciones oficiales; y l) prueba de no alteración.

La fe pública criptográfica constituye una capa técnica de integridad, autenticidad y evidencia. No sustituirá por sí misma la fe pública notarial, registral o administrativa, ni las formalidades constitutivas, controles de legalidad o competencias profesionales exigidas por el ordenamiento jurídico.

La valoración de su eficacia probatoria corresponderá a la autoridad competente de acuerdo con las reglas sustantivas y procesales aplicables.

Artículo 355. Fedatarios y Fe Pública Criptográfica

Los notarios públicos, registradores, jueces, funcionarios autorizados y demás fedatarios podrán utilizar herramientas de fe pública criptográfica para fortalecer la autenticidad, integridad, trazabilidad y conservación de actos bajo su competencia.

El uso de fe pública criptográfica deberá respetar normativa notarial, registral, judicial, administrativa, protección de datos, identidad digital soberana, firma digital y seguridad de llaves.

Artículo 356. Valor Probatorio de la Fe Pública Criptográfica

Los registros, hashes, sellos de tiempo, firmas criptográficas, certificados verificables, pruebas de conocimiento cero y evidencias generadas mediante sistemas autorizados o reconocidos podrán tener valor probatorio conforme a la ley.

La valoración judicial o administrativa deberá considerar autenticidad, integridad, cadena de custodia digital, fiabilidad del sistema, control de llaves, auditoría, trazabilidad y ausencia de manipulación.

SECCIÓN IV — SMART CONTRACTS REGISTRALES Y ESTATALES

Artículo 357. Reconocimiento Jurídico de Smart Contracts Registrales

Se reconocen los smart contracts registrales como mecanismos tecnológicos destinados a automatizar, verificar, ejecutar o registrar actos jurídicos, condiciones, plazos, pagos, gravámenes, transferencias, certificaciones o eventos vinculados al Registro Público y demás registros oficiales.

Su validez dependerá de su conformidad con la ley, capacidad de las partes, consentimiento, objeto lícito, forma exigida, control registral, debido proceso y demás requisitos del acto subyacente.

Artículo 358. Automatización de Actos Registrales

Los smart contracts registrales podrán utilizarse para automatizar procesos previamente definidos, tales como:

a) Control de prelación registral.
b) Registro de condiciones suspensivas.
c) Cancelación de gravámenes cumplidos.
d) Seguimiento de plazos.
e) Emisión de certificaciones verificables.
f) Notificaciones registrales.
g) Liquidación de derechos o tasas.
h) Interoperabilidad con catastro.
i) Ejecución de garantías programables.
j) Tokenización registral.
k) Actualización de estados registrales.

Artículo 359. Límites a la Automatización Jurídica

Ningún smart contract registral podrá eliminar garantías de debido proceso, derecho de defensa, revisión humana, control registral, tutela judicial efectiva o protección de terceros.

No podrán automatizarse de forma irreversible actos que requieran valoración jurídica compleja, consentimiento disputado, afectación de terceros, control judicial, medidas cautelares o resolución de controversias, salvo regulación expresa y garantías suficientes.

Artículo 360. Supervisión Humana y Control Registral

Todo sistema de smart contracts estatales o registrales deberá contar con supervisión humana competente, mecanismos de suspensión, revisión, auditoría, corrección de errores, control de acceso, gestión de llaves y responsabilidad institucional.

El Estado deberá identificar claramente la autoridad responsable del diseño, operación, actualización, auditoría y corrección de dichos sistemas.

SECCIÓN V — PROPIEDAD PROGRAMABLE Y TOKENIZACIÓN REGISTRAL

Artículo 361. Propiedad Programable

Se reconoce la propiedad programable como la representación jurídica y tecnológica de derechos patrimoniales mediante sistemas digitales capaces de ejecutar condiciones, transferencias, restricciones, gravámenes, uso, usufructo, garantía, fraccionamiento o trazabilidad conforme a ley.

La propiedad programable deberá respetar propiedad privada, seguridad jurídica, publicidad registral, derechos de terceros, debido proceso y límites legales aplicables.

Artículo 362. Tokenización Registral

Los derechos inscribibles podrán representarse mediante tokens cuando la ley lo permita y exista vinculación verificable con el registro correspondiente.

La tokenización registral deberá garantizar:

a) Identificación del derecho.
b) Titularidad registral.
c) Correspondencia entre token y asiento.
d) Prevención de doble emisión.
e) Gravámenes visibles.
f) Reglas de transferencia.
g) Protección de terceros.
h) Mecanismos de bloqueo judicial o administrativo.
i) Interoperabilidad con notariado y catastro.
j) Privacidad de datos personales.

Artículo 363. Gravámenes y Garantías Tokenizadas

Podrán representarse mediante blockchain o tokens gravámenes, garantías mobiliarias, hipotecas, prendas, fideicomisos de garantía, anotaciones, embargos, medidas cautelares y demás cargas patrimoniales permitidas por ley.

La representación tokenizada de gravámenes deberá asegurar publicidad, oponibilidad, prelación, trazabilidad, cancelación legítima y protección de acreedores y terceros.

Artículo 364. Fraccionamiento Registral Digital

El fraccionamiento digital de derechos registrables será permitido únicamente cuando la ley sustantiva permita copropiedad, participación, cuotas, fideicomisos, derechos económicos o estructuras equivalentes.

El fraccionamiento no podrá utilizarse para evadir normas urbanísticas, registrales, fiscales, societarias, de valores, sucesorias o de protección al consumidor.

SECCIÓN VI — NOTARIADO DIGITAL E INTEROPERABILIDAD

Artículo 365. Notariado Digital Blockchain-Compatible

El notariado costarricense podrá interoperar con infraestructura blockchain, credenciales verificables, sellos criptográficos, firma digital, identidad soberana, smart contracts y Registro Público blockchain.

Los notarios podrán utilizar herramientas tecnológicas para:

a) Anclar escrituras o testimonios.
b) Verificar identidad digital.
c) Registrar hashes documentales.
d) Emitir certificaciones verificables.
e) Validar consentimiento.
f) Verificar titularidad de wallets.
g) Integrar smart contracts con contratos legales.
h) Preservar evidencia digital.

Artículo 366. Firma Digital, Firma Criptográfica y Credenciales Verificables

El Estado reconocerá la interoperabilidad entre firma digital, firma criptográfica, credenciales verificables, identidad digital soberana y sellos de tiempo, conforme a los requisitos de autenticidad, consentimiento, integridad y capacidad legal.

La ley podrá establecer niveles de confianza diferenciados según el acto, riesgo, materia, cuantía o efecto jurídico.

Artículo 367. Interoperabilidad con Catastro, Municipalidades y Autoridades

El Registro Público blockchain deberá interoperar progresivamente con Catastro, municipalidades, autoridades tributarias, ambientales, judiciales, notariales y administrativas para fortalecer trazabilidad territorial, permisos, uso de suelo, impuestos, gravámenes y titularidad.

La interoperabilidad deberá impedir superposición indebida de planos, permisos opacos, manipulación territorial y corrupción administrativa.

SECCIÓN VII — TRANSPARENCIA, PRIVACIDAD Y SEGURIDAD REGISTRAL

Artículo 368. Transparencia Registral Verificable

Toda persona podrá verificar la integridad de actos registrales públicos mediante mecanismos técnicos accesibles, sin necesidad de acceder a datos personales sensibles.

El Estado deberá proveer exploradores, APIs, certificados verificables, consultas de integridad y herramientas de auditoría registral.

Artículo 369. Protección de Datos Sensibles en Registros Blockchain

No deberán publicarse en blockchain pública datos personales sensibles, información patrimonial innecesaria, datos biométricos, datos familiares, datos financieros protegidos o información cuya exposición irreversible pueda afectar derechos fundamentales.

Se preferirá el uso de hashes, referencias, pruebas criptográficas, credenciales verificables, permisos de acceso, almacenamiento off-chain seguro y mecanismos de minimización.

Artículo 370. Ciberseguridad Registral

El Registro Público blockchain deberá cumplir estándares reforzados de ciberseguridad, gestión de llaves, continuidad operativa, respaldo, criptoagilidad, seguridad post-cuántica, auditoría de smart contracts, control de proveedores y respuesta a incidentes.

SECCIÓN VIII — CLÁUSULAS CONSTITUCIONALES FINALES

Artículo 371. Cláusula de Seguridad Jurídica Digital

Toda infraestructura registral digital deberá interpretarse y aplicarse conforme a la seguridad jurídica, protección de propiedad, integridad documental, trazabilidad, publicidad registral, debido proceso, privacidad, interoperabilidad y tutela judicial efectiva.

Artículo 372. Cláusula Anticorrupción Registral

Será contrario al interés público todo sistema registral que permita alteraciones invisibles, eliminación de historial, opacidad de modificaciones, dependencia tecnológica no auditable, centralización indebida de llaves, bloqueo de auditoría o imposibilidad de verificar integridad documental.

Artículo 373. Cláusula de Propiedad Digital Soberana

Toda persona tiene derecho a que sus derechos patrimoniales, registrales, tokenizados o programables sean reconocidos, protegidos, transferibles, verificables y defendibles conforme a ley, sin discriminación por su forma digital, criptográfica o tokenizada.

La propiedad digital soberana deberá protegerse frente a confiscación arbitraria, manipulación registral, censura tecnológica, pérdida de acceso injustificada, intermediación obligatoria indebida y dependencia de sistemas cerrados.

CAPÍTULO XIII — RÉGIMEN TRIBUTARIO DIGITAL, SOBERANÍA FISCAL E INCENTIVOS PARA LA ECONOMÍA DESCENTRALIZADA

SECCIÓN I — PRINCIPIOS TRIBUTARIOS DIGITALES

Artículo 374. Neutralidad Tecnológica Tributaria

La tributación de activos digitales, tokenización, Bitcoin, stablecoins, DeFi, minería, staking, validación, DAOs, RWA y demás actividades Web3 deberá aplicarse conforme a su sustancia económica, no por el solo hecho de utilizar blockchain, smart contracts, criptografía o infraestructura descentralizada.

La forma tecnológica de representación, custodia o transferencia no deberá generar una carga tributaria más gravosa que una operación económicamente equivalente realizada mediante medios tradicionales.

Artículo 375. Seguridad Jurídica Fiscal Digital

El Estado deberá establecer reglas claras, previsibles y técnicamente aplicables sobre los hechos generadores, base imponible, momento de reconocimiento, documentación, valoración y obligaciones formales aplicables a activos digitales y economía descentralizada.

No podrán imponerse obligaciones fiscales imposibles de cumplir por la naturaleza descentralizada, pseudónima, global o no custodial de la tecnología.

Artículo 376. Proporcionalidad Tributaria

Las obligaciones fiscales digitales deberán ser proporcionales al tipo de usuario, actividad, volumen, habitualidad, organización empresarial, jurisdicción, fuente de renta, nivel de intermediación y capacidad real de cumplimiento.

No deberá tratarse igual a:

a) Usuario minorista en autocustodia.
b) Trader profesional.
c) VASP.
d) Emisor de tokens.
e) Banco digital.
f) DAO.
g) Minero.
h) Validador.
i) Inversionista institucional.
j) Plataforma de tokenización.
k) Desarrollador de software.

Artículo 377. Prohibición de Tributación Confiscatoria Digital

Queda prohibida toda carga fiscal, obligación formal, retención, sanción o interpretación administrativa que, directa o indirectamente, haga inviable la autocustodia, la innovación Web3, la operación de nodos, la tokenización legítima, el uso de Bitcoin, el desarrollo de software, la actividad DeFi o la participación en mercados digitales lícitos.

SECCIÓN II — BITCOIN Y ACTIVOS DIGITALES DESCENTRALIZADOS

Artículo 378. Bitcoin como Activo Financiero Digital Descentralizado

Para efectos tributarios, Bitcoin será reconocido como activo financiero digital descentralizado, sin emisor, sin administrador central y sin promesa de rendimiento de terceros.

La tenencia pasiva de Bitcoin no constituirá por sí sola hecho generador de impuesto.

La apreciación no realizada de Bitcoin o activos digitales descentralizados no estará sujeta a imposición mientras no exista enajenación, conversión, realización económica, intercambio oneroso, pago, distribución o evento tributario expresamente establecido por ley.

Artículo 379. Exención de Bitcoin Adquirido Descentralizadamente fuera de Costa Rica

Las ganancias derivadas de Bitcoin adquirido, recibido, minado, transferido o mantenido mediante infraestructura descentralizada fuera del territorio costarricense, sin intermediario domiciliado en Costa Rica y bajo autocustodia personal, estarán exentas de tributación en Costa Rica cuando no provengan de fuente costarricense, actividad empresarial local, prestación de servicios en Costa Rica, trading profesional domiciliado o estructura destinada a eludir obligaciones fiscales nacionales.

Esta exención no aplicará cuando:

a) Bitcoin sea recibido como pago por servicios prestados en Costa Rica.
b) Exista actividad habitual, profesional o empresarial desde Costa Rica.
c) Se utilice una entidad costarricense como vehículo de inversión.
d) La operación esté vinculada a fuente costarricense.
e) Exista simulación, abuso, fraude o elusión.
f) Se trate de intermediación, custodia o servicios a terceros.

Artículo 380. Tributación de Ganancias de Capital Digitales

Las ganancias de capital provenientes de la enajenación de activos digitales estarán sujetas al régimen fiscal aplicable únicamente cuando exista realización económica conforme a ley.

Se considerarán eventos potencialmente realizables:

a) Venta por moneda fiduciaria.
b) Intercambio por otro activo digital con ganancia realizada, cuando sea determinable.
c) Uso como pago de bienes o servicios.
d) Redención contra emisor.
e) Liquidación en mercado secundario.
f) Transferencia onerosa.
g) Distribución de beneficios.

No constituirán realización por sí solos:

a) Transferencias entre wallets propias.
b) Migración entre redes.
c) Cambio de custodia a autocustodia.
d) Puentes técnicos sin disposición económica.
e) Reorganizaciones técnicas de protocolo.
f) Actualizaciones de token sin cambio económico sustancial.
g) Tenencia pasiva.

Artículo 381. Tributación de Trading Profesional

La actividad habitual, organizada, profesional o empresarial de compraventa de activos digitales realizada desde Costa Rica podrá estar sujeta al régimen tributario aplicable a actividades lucrativas o empresariales.

Para determinar habitualidad se considerarán:

a) Frecuencia.
b) Volumen.
c) Organización empresarial.
d) Uso de infraestructura profesional.
e) Publicidad de servicios.
f) Administración de fondos de terceros.
g) Personal contratado.
h) Registro como actividad económica.
i) Intención comercial predominante.

La simple inversión personal, ahorro, tenencia o rebalanceo ocasional de portafolio no deberá presumirse actividad empresarial.

SECCIÓN III — TOKENIZACIÓN Y MERCADOS DIGITALES

Artículo 382. Tributación de Tokenización de Activos

La tokenización de un activo no generará por sí sola impuesto cuando no implique transmisión económica, realización de ganancia, cambio de titularidad efectiva, distribución de beneficios o acto gravado conforme a ley.

El hecho imponible dependerá del acto subyacente: venta, arrendamiento, cesión, dividendos, intereses, regalías, rendimientos, servicios, transmisión patrimonial o realización económica equivalente.

Artículo 383. Tributación de Mercados Secundarios

Las operaciones realizadas en mercados secundarios de activos digitales estarán sujetas al tratamiento fiscal que corresponda según la naturaleza del activo, residencia del contribuyente, fuente de renta, lugar de actividad económica, tipo de operación y realización efectiva.

Las plataformas autorizadas podrán actuar como agentes de información o retención únicamente cuando exista base legal clara, capacidad técnica real y proporcionalidad.

Artículo 384. Tratamiento Fiscal de Stablecoins

Las stablecoins utilizadas como medio de pago, liquidación o resguardo operativo no generarán impuesto por su mera tenencia.

La conversión, redención, rendimiento, uso comercial, diferencia cambiaria, intereses, recompensas o ganancias asociadas a stablecoins podrán tributar conforme a su naturaleza económica y régimen aplicable.

Las stablecoins no serán tratadas automáticamente como depósitos bancarios, dinero electrónico, títulos valores o instrumentos de inversión por su sola existencia.

Artículo 385. Tributación de RWA

Los tokens representativos de activos reales estarán sujetos al régimen fiscal aplicable al activo subyacente o derecho económico representado.

La tributación podrá corresponder a:

a) Bienes inmuebles.
b) Participaciones corporativas.
c) Instrumentos de deuda.
d) Facturas.
e) Regalías.
f) Derechos ambientales.
g) Ingresos productivos.
h) Arrendamientos.
i) Rendimientos financieros.
j) Ganancias de capital.

La tokenización no deberá utilizarse para evadir impuestos aplicables al subyacente ni para crear doble imposición injustificada.

SECCIÓN IV — STAKING, MINERÍA, VALIDADORES Y NODOS

Artículo 386. Tributación de Staking

Los ingresos derivados de staking podrán estar sujetos a tributación cuando constituyan rendimiento efectivamente recibido, disponible y económicamente realizable por el contribuyente.

Deberá distinguirse entre:

a) Staking propio no profesional.
b) Staking profesional.
c) Staking-as-a-service.
d) Validación delegada.
e) Recompensas ilíquidas o bloqueadas.

f) Recompensas sujetas a slashing o riesgo técnico.
g) Distribuciones de terceros.

La mera delegación técnica o participación en consenso no deberá ser tratada automáticamente como actividad empresarial.

Artículo 387. Tributación de Minería

La minería de activos digitales podrá ser tratada como actividad económica cuando se realice de forma habitual, organizada, comercial o empresarial desde territorio costarricense.

La determinación fiscal deberá considerar:

a) Ubicación de equipos.
b) Consumo energético.
c) Organización empresarial.
d) Venta de activos minados.
e) Costos deducibles.
f) Ingresos efectivamente realizados.
g) Valoración razonable al momento de recepción o disposición.
h) Impacto ambiental y energético.

La minería individual, experimental, académica o de baja escala podrá recibir tratamiento simplificado.

Artículo 388. Tributación de Validadores y Nodos

La operación de nodos o validadores no constituirá por sí sola hecho generador tributario si no produce ingresos, comisiones, recompensas o actividad económica gravable.

Cuando existan ingresos por validación, comisiones, recompensas, servicios de infraestructura o participación profesional, se aplicará el régimen fiscal correspondiente según actividad, fuente, residencia y realización económica.

SECCIÓN V — DAOs Y ECONOMÍA DESCENTRALIZADA

Artículo 389. Régimen Tributario de DAOs

Las DAOs podrán estar sujetas a tratamiento tributario conforme a su estructura, personalidad jurídica, lugar de administración efectiva, fuente de ingresos, actividad económica, tesorería, miembros, control, residencia fiscal y operaciones realizadas.

La IID y la autoridad tributaria podrán establecer categorías diferenciadas para:

a) DAOs sin personalidad jurídica.
b) DAOs registradas en Costa Rica.
c) DAOs extranjeras con actividad local.
d) DAOs de inversión.
e) DAOs de protocolo.
f) DAOs de comunidad.
g) DAOs con tesorería activa.
h) DAOs sin distribución de beneficios.

Artículo 390. Tesorerías Descentralizadas

Las tesorerías de DAOs, protocolos o comunidades digitales deberán recibir tratamiento fiscal conforme a titularidad, administración, control, distribución, uso de fondos, residencia y finalidad económica.

La mera existencia de una tesorería on-chain no implicará por sí sola renta gravable para sus miembros mientras no exista distribución, beneficio económico individualizado, retiro, pago o asignación patrimonial.

Artículo 391. Governance Tokens

La recepción, tenencia o participación en governance tokens no constituirá renta gravable por sí sola, salvo que exista valor económico realizado, venta, distribución, rendimiento, compensación por servicios, asignación remuneratoria o beneficio patrimonial determinable.

SECCIÓN VI — INCENTIVOS ESTRATÉGICOS PAÍS WEB3

Artículo 392. Incentivos para Innovación Web3

El Estado podrá establecer incentivos tributarios, administrativos o regulatorios para proyectos que desarrollen infraestructura Web3, blockchain, identidad soberana, ciberseguridad, IA descentralizada, tokenización, DeFi, compliance criptográfico, educación tecnológica o servicios digitales exportables desde Costa Rica.

Artículo 393. Incentivos para Infraestructura Blockchain

Podrán establecerse incentivos para inversión en nodos, validadores, centros de datos, infraestructura post-cuántica, auditoría de smart contracts, investigación criptográfica, seguridad blockchain, open-source y redes descentralizadas.

Artículo 394. Incentivos para IA, Blockchain y Computación Avanzada

El Estado podrá promover incentivos para empresas, universidades, startups y centros de investigación que desarrollen IA segura, blockchain, criptografía post-cuántica, ZKP, privacidad, seguridad digital, soberanía computacional y auditoría algorítmica.

Artículo 395. Incentivos para Exportación de Servicios Digitales

Los servicios digitales, legales, tecnológicos, financieros, educativos, de software, auditoría, compliance, tokenización, IA, blockchain y ciberseguridad exportados desde Costa Rica podrán recibir tratamiento competitivo conforme a regímenes de promoción, zonas francas, incentivos de innovación o normas especiales.

SECCIÓN VII — SOBERANÍA FISCAL INTELIGENTE

Artículo 396. Coordinación Internacional

Costa Rica podrá coordinar con organismos internacionales, autoridades fiscales extranjeras y estándares globales para evitar doble imposición, evasión, abuso, lavado de dinero y estructuras ilícitas, sin renunciar a su modelo de libertad financiera digital, autocustodia y competitividad Web3.

Artículo 397. AML/CFT sin Destrucción de Innovación Fiscal

Las obligaciones fiscales y AML/CFT deberán aplicarse de forma coordinada, proporcional y basada en riesgo, sin transformar la administración tributaria en mecanismo de vigilancia financiera masiva.

La información requerida deberá limitarse a lo necesario, con garantías de privacidad, debido proceso, protección de datos y seguridad.

Artículo 398. Tributación Basada en Actividad Económica Real

La autoridad tributaria deberá determinar obligaciones fiscales sobre la base de actividad económica real, fuente de renta, residencia, realización, habitualidad, organización empresarial y beneficio económico efectivo.

No podrá presumirse renta por:

a) Tenencia pasiva.
b) Autocustodia.
c) Transferencias entre wallets propias.
d) Participación técnica en redes.
e) Uso de privacidad legítima.
f) Participación en governance sin beneficio económico.
g) Pruebas técnicas.
h) Interacciones sin realización económica.

Artículo 399. Protección de Autocustodia frente a Sobrerregulación Fiscal

La autoridad tributaria no podrá imponer obligaciones de reporte, valoración, retención, intermediación o documentación que hagan inviable la autocustodia legítima o que obliguen indirectamente a utilizar custodios, exchanges, bancos o intermediarios.

Los deberes de información deberán ser razonables, proporcionales y técnicamente cumplibles.

SECCIÓN VIII — CLÁUSULAS CONSTITUCIONALES FINALES

Artículo 400. Cláusula de Libertad Financiera Tributaria

Toda norma tributaria relacionada con activos digitales deberá interpretarse conforme a libertad financiera digital, propiedad privada, territorialidad, seguridad jurídica, autocustodia, neutralidad tecnológica, proporcionalidad y competitividad nacional.

Artículo 401. Cláusula Anti-Debanking Fiscal

Ninguna interpretación fiscal podrá utilizarse para justificar exclusión bancaria automática, cierre de cuentas, bloqueo financiero, negativa de servicios o discriminación contra personas o empresas que participen lícitamente en la economía digital.

Artículo 402. Cláusula de Competitividad Digital Nacional

La política tributaria sobre activos digitales deberá promover la competitividad internacional de Costa Rica como Hub de tecnologías descentralizadas y emergentes, evitando doble imposición, inseguridad jurídica, cargas desproporcionadas, obligaciones imposibles, discriminación tecnológica y fuga de talento.

CAPÍTULO XIV — SOBERANÍA FINANCIERA DIGITAL, TERRITORIALIDAD FISCAL, FINANCIAMIENTO REGULATORIO Y ZONA FRANCA TECNOLÓGICA WEB3

SECCIÓN I — SOBERANÍA FINANCIERA DIGITAL Y TERRITORIALIDAD FISCAL

Artículo 403. Principio de Soberanía Financiera Digital

Toda persona tiene derecho a poseer, custodiar, transferir, ahorrar e invertir en activos digitales descentralizados, incluyendo Bitcoin, mediante autocustodia, sin que la mera tenencia, apreciación no realizada o control directo sobre llaves privadas constituya hecho generador tributario.

La soberanía financiera digital comprende la facultad de mantener patrimonio digital propio fuera de intermediarios, custodios, bancos o plataformas centralizadas, siempre que no exista actividad ilícita, simulación, fraude, captación pública o fuente costarricense gravable.

Artículo 404. Principio de Territorialidad Fiscal Digital

La tributación de activos digitales en Costa Rica deberá respetar el principio de territorialidad fiscal, gravando únicamente rentas, ganancias, servicios, actividades económicas o hechos generadores atribuibles al territorio costarricense conforme a la ley.

No se considerará renta de fuente costarricense la mera tenencia, apreciación, transferencia entre wallets propias o custodia personal de activos digitales descentralizados adquiridos, mantenidos o gestionados fuera de Costa Rica sin intermediario, servicio, emisor, plataforma o actividad económica domiciliada en el país.

Artículo 405. Regla Especial para Bitcoin Descentralizado

Bitcoin, por su naturaleza de activo digital descentralizado, sin emisor, sin administrador central, sin promesa de rendimiento y sin fuente territorial atribuible por su mera existencia, no estará sujeto a tributación en Costa Rica por simple tenencia, apreciación no realizada, autocustodia o adquisición descentralizada fuera del territorio nacional.

Sí podrá existir obligación tributaria cuando Bitcoin sea utilizado para:

a) Pago por servicios prestados en Costa Rica.
b) Pago por bienes vendidos desde Costa Rica.
c) Actividad empresarial organizada en Costa Rica.
d) Trading profesional realizado desde Costa Rica.
e) Intermediación, custodia o servicios a terceros.
f) Conversión con ganancia atribuible a fuente costarricense.
g) Operaciones realizadas mediante entidad domiciliada en Costa Rica.
h) Simulación, abuso o elusión fiscal.

Artículo 406. Ganancias de Capital en Protocolos, Tokens y Criptoactivos con Fuente Costarricense

Las ganancias de capital o rentas derivadas de protocolos, tokens, activos digitales, stablecoins, RWA, security tokens, governance tokens, tokens de utilidad, DeFi o instrumentos tokenizados estarán sujetas a tributación cuando la ganancia sea atribuible a fuente costarricense, actividad económica desarrollada en Costa Rica, entidad domiciliada, servicio prestado desde Costa Rica, mercado regulado nacional o plataforma bajo jurisdicción costarricense.

La autoridad tributaria deberá distinguir entre:

a) Usuario personal en autocustodia.
b) Inversionista pasivo.
c) Trading profesional.
d) Emisor de tokens.
e) Plataforma regulada.
f) VASP.
g) Banco digital.
h) DAO con actividad local.
i) Tokenización de activo costarricense.
j) Actividad empresarial organizada.

Artículo 407. Prohibición de Gravar Movimientos Técnicos sin Realización Económica

No constituirán hecho generador tributario por sí solos:

a) Transferencias entre wallets propias.
b) Cambio de wallet.
c) Cambio de custodia a autocustodia.

d) Migración técnica de tokens.
e) Puentes entre redes sin disposición económica.
f) Actualizaciones de protocolo.
g) Reemplazo técnico de token sin beneficio económico.
h) Participación en gobernanza sin remuneración.
i) Firma de transacciones sin transferencia patrimonial real.
j) Tenencia pasiva.

Artículo 408. Cláusula Antiabuso y Antisimulación

La protección fiscal de la autocustodia, Bitcoin descentralizado y territorialidad digital no amparará esquemas de simulación, abuso, fraude, ocultamiento de fuente costarricense, intermediación encubierta, captación pública no registrada, lavado de dinero, evasión tributaria o elusión artificial.

La autoridad competente podrá recalificar operaciones conforme a sustancia económica, debido proceso, prueba suficiente, proporcionalidad y derecho de defensa.

SECCIÓN II — MODELO DE FINANCIAMIENTO REGULATORIO DE LA IID

Artículo 409. Principio de Financiamiento Regulatorio Proporcional

Las funciones especializadas de la IID podrán financiarse mediante asignaciones presupuestarias y, en proporción razonable al costo de regulación y supervisión, mediante tasas, derechos de registro y licenciamiento, autorizaciones, servicios técnicos y demás ingresos legalmente permitidos.

El modelo de financiamiento no podrá trasladar cargas fiscales generalizadas a usuarios personales, autocustodia, tenencia pasiva de activos digitales ni actividades tecnológicas no reguladas. Todos los recursos se incorporarán al Presupuesto Nacional y estarán sujetos a los controles de Hacienda Pública aplicables.

Artículo 410. Fuentes de Financiamiento de la IID

La IID podrá contar, conforme a ley, con recursos provenientes de: a) tasas de licenciamiento VASP; b) tasas de renovación; c) autorizaciones de bolsas de activos digitales; d) licencias de bancos digitales blockchain-native; e) registros de emisores; f) autorizaciones de tokenización institucional; g) derechos por aprobación de white papers cuando corresponda; h) supervisión de emisores de stablecoins; i) certificaciones de compliance criptográfico; j) autorizaciones de sandboxes; k) licencias de custodios; l) registros de DAOs; m) tasas de mercados secundarios; n) servicios técnicos de clasificación; o) multas y sanciones; p) cooperación internacional no condicionada; y q) asignaciones iniciales o transferencias presupuestarias autorizadas.

La percepción y utilización de estos recursos se sujetará a la Ley N.° 9524, a la Ley de Administración Financiera de la República y Presupuestos Públicos y a las demás normas de presupuesto, tesorería, control interno y fiscalización aplicables.

Artículo 411. Tasas Proporcionales y No Confiscatorias

Las tasas regulatorias deberán responder al costo razonable de los servicios de registro, licenciamiento, supervisión o fiscalización que las justifiquen y serán proporcionales al tamaño, riesgo, volumen, tipo de actividad, custodia, impacto sistémico y capacidad económica del sujeto regulado.

La ley y sus anexos reglamentarios deberán establecer la base, parámetros objetivos, sujetos obligados y límites máximos aplicables. La IID podrá aplicar y actualizar las fórmulas técnicas dentro de esos límites, pero no crear nuevas tasas, hechos generadores o sujetos pasivos mediante circular, guía o acto administrativo.

Queda prohibido fijar tasas que impidan la entrada de startups, favorezcan monopolios, excluyan innovación local o conviertan la licencia en privilegio de grandes actores internacionales.

Artículo 412. Programa de Supervisión e Innovación Digital

Créase, dentro del programa presupuestario individualizado de la IID, el Programa de Supervisión e Innovación Digital como mecanismo de asignación, identificación y trazabilidad de recursos destinados a: a) supervisión técnica; b) auditoría blockchain; c) ciberseguridad; d) educación financiera digital; e) sandboxes; f) investigación en ZKP, IA y tecnologías post-cuánticas; g) infraestructura pública blockchain; h) protección de usuarios; i) cooperación internacional; j) herramientas de compliance criptográfico; y k) formación de talento nacional.

El Programa no tendrá personalidad jurídica ni patrimonio separados de la Administración Central. Su ejecución deberá sujetarse al Presupuesto Nacional, control interno, fiscalización pública, auditoría externa cuando corresponda y mecanismos de transparencia y trazabilidad de ingresos, egresos y contrataciones relevantes.

Artículo 412 bis. Régimen Presupuestario de la IID

La IID contará con un programa presupuestario individualizado que permita identificar, administrar y fiscalizar los recursos destinados al ejercicio de sus competencias.

Sus ingresos, presupuestos y gastos se incorporarán al Presupuesto Nacional y se administrarán de conformidad con la Ley N.° 9524, la Ley de Administración Financiera de la República y Presupuestos Públicos y demás normativa aplicable. La personalidad jurídica instrumental prevista en esta ley no excluye dichos controles ni crea un patrimonio separado propio de una institución autónoma.

La integración al Presupuesto Nacional no facultará al MICITT para condicionar decisiones regulatorias individuales ni utilizar asignaciones, modificaciones administrativas o actos de ejecución presupuestaria como mecanismo de interferencia en las competencias legalmente desconcentradas.

Las tasas, cánones y contribuciones regulatorias deberán observar proporcionalidad, transparencia, razonabilidad, relación con el costo de supervisión, no confiscatoriedad y prevención de barreras artificiales de entrada.

Artículo 412 ter. Fondo Nacional de Soberanía Digital e Innovación Tecnológica

Créase el Fondo Nacional de Soberanía Digital e Innovación Tecnológica como mecanismo presupuestario estratégico para fortalecer el desarrollo de la economía digital costarricense, la industria descentralizada, la infraestructura digital estratégica y la competitividad tecnológica nacional, sin personalidad jurídica propia ni separación del régimen presupuestario del Gobierno Central.

El Fondo tendrá por finalidad financiar infraestructura digital estratégica, interoperabilidad institucional, ciberseguridad, investigación tecnológica, inteligencia artificial, hubs digitales, centros de datos, blockchain estatal, identidad digital soberana, formación tecnológica, resiliencia digital, sandboxes regulatorios, tokenización económica y proyectos de modernización institucional vinculados con soberanía digital.

La recaudación tributaria continuará bajo rectoría del Ministerio de Hacienda conforme al marco constitucional, presupuestario y fiscal costarricense. La IID no tendrá facultades tributarias ni sustituirá competencias presupuestarias, financieras o de control constitucionalmente atribuidas a otras autoridades.

La ley podrá destinar recursos legalmente definidos al fortalecimiento del ecosistema nacional de soberanía digital conforme a las reglas del Presupuesto Nacional, control fiscal, transparencia, evaluación de impacto y protección del interés público. La IID actuará únicamente como órgano técnico especializado, evaluador, coordinador y supervisor técnico de los proyectos dentro de sus competencias, sin sustituir al Ministerio de Hacienda, a la Contraloría General de la República ni a las autoridades presupuestarias competentes.

Artículo 413. Prohibición de Captura Financiera del Regulador

El financiamiento de la IID no podrá generar dependencia indebida de un grupo reducido de regulados, bancos, exchanges, emisores, proveedores tecnológicos o actores internacionales.

La ley establecerá límites, transparencia, auditoría, incompatibilidades y mecanismos anticaptura.

SECCIÓN III — RÉGIMEN ESPECIAL DE ZONA FRANCA TECNOLÓGICA Y DIGITAL

Artículo 414. Creación del Régimen Especial de Zona Franca Tecnológica y Digital

Créase el Régimen Especial de Zona Franca Tecnológica y Digital como marco de incentivos para empresas, centros de investigación, startups, fundaciones, DAOs registradas, laboratorios, proveedores de infraestructura y actores tecnológicos que desarrollen actividades estratégicas de economía digital avanzada desde Costa Rica.

Este régimen podrá coexistir con el régimen general de zonas francas, o integrarse como subcategoría especializada conforme a la ley.

Artículo 415. Actividades Elegibles

Podrán acogerse al Régimen Especial de Zona Franca Tecnológica y Digital las actividades relacionadas con:

a) Blockchain.
b) Web3 y Web4.
c) Tokenización.
d) Infraestructura DeFi.
e) IA y automatización.
f) Ciberseguridad.
g) Criptografía post-cuántica.
h) ZKP.
i) Identidad digital soberana.
j) Auditoría de smart contracts.
k) Compliance criptográfico.
l) Infraestructura cloud soberana.
m) Centros de datos.
n) Validadores y nodos.
o) Desarrollo de wallets.
p) Infraestructura de mercados digitales.
q) Stablecoin infrastructure.
r) RWA platforms.
s) Software open-source.
t) Exportación de servicios digitales.
u) Investigación y desarrollo tecnológico.
v) Educación tecnológica especializada.

Artículo 416. Beneficios Fiscales del Régimen Tecnológico

Las empresas acogidas al Régimen Especial de Zona Franca Tecnológica y Digital podrán acceder, conforme a los requisitos, porcentajes, plazos y límites establecidos por esta ley y la legislación tributaria aplicable, a beneficios fiscales sobre actividades elegibles de exportación, innovación, investigación, desarrollo e infraestructura tecnológica.

Los beneficios podrán comprender, cuando exista habilitación legal expresa: a) impuesto sobre la renta por actividades elegibles; b) impuesto al valor agregado sobre operaciones calificadas; c) derechos e impuestos de importación sobre hardware, servidores, equipos de seguridad, infraestructura tecnológica y equipos de investigación; d) retenciones sobre pagos tecnológicos internacionales en los supuestos legalmente autorizados; e) reinversión en investigación, desarrollo e infraestructura; y f) otros incentivos nacionales expresamente definidos por ley.

Los tributos municipales y sus eventuales exoneraciones, reducciones o incentivos únicamente podrán ser afectados cuando exista habilitación legal y se cumplan los procedimientos constitucionales, legales y municipales aplicables. La presente ley no crea por sí sola una exoneración de tributos municipales.

Todo beneficio estará condicionado a sustancia económica, actividad real, cumplimiento fiscal, inversión verificable, generación de valor, ausencia de simulación y los demás requisitos del régimen.

Artículo 417. Incentivos Especiales para Infraestructura Descentralizada

Podrán establecerse incentivos adicionales para proyectos que desarrollen infraestructura descentralizada de alto valor estratégico, incluyendo:

a) Nodos institucionales.
b) Validadores.
c) Infraestructura ZKP.
d) Criptografía post-cuántica.
e) Herramientas open-source.
f) Protocolos de identidad soberana.
g) Seguridad blockchain.
h) Compliance criptográfico.
i) Infraestructura de tokenización RWA.
j) Sistemas de auditoría on-chain.
k) Infraestructura electoral verificable.
l) Registro Público blockchain.

Artículo 418. Sustancia Económica y Arraigo Nacional

Para acceder a beneficios, los beneficiarios deberán demostrar sustancia económica real en Costa Rica, incluyendo según corresponda:

a) Personal calificado local.
b) Oficinas o infraestructura operativa.
c) Desarrollo tecnológico efectivo.
d) Inversión mínima.
e) Transferencia de conocimiento.
f) Programas de capacitación.
g) Contratación de talento costarricense.
h) Vinculación con universidades.
i) Exportación de servicios.
j) Investigación y desarrollo.
k) Gobernanza transparente.

Artículo 419. Régimen Especial para Startups Web3

Se establecerá un régimen simplificado para startups Web3, IA, blockchain, ciberseguridad y tokenización, con requisitos proporcionales de entrada, licenciamiento reducido, ventanilla única, acompañamiento regulatorio y acceso a sandbox.

Las startups podrán recibir beneficios escalonados según crecimiento, inversión, riesgo, volumen, empleo, exportación y actividad regulada.

Artículo 420. Ventanilla Única Web3

Créase la Ventanilla Única Web3 para centralizar trámites de incorporación, licenciamiento, zona franca tecnológica, sandbox, registros IID, permisos migratorios especializados, certificaciones, incentivos y coordinación institucional.

Artículo 421. Talento, Migración e Innovación

El régimen podrá incluir facilidades migratorias para fundadores, desarrolladores, investigadores, expertos en ciberseguridad, criptógrafos, auditores de smart contracts, especialistas en IA, operadores de infraestructura y profesionales estratégicos.

También promoverá formación de talento costarricense mediante becas, convenios universitarios, programas técnicos, investigación aplicada y certificaciones.

SECCIÓN IV — VENTAJA COMPETITIVA FRENTE A EL SALVADOR Y OTROS HUBS

Artículo 422. Modelo Costarricense de Hub Web3 Democrático

Costa Rica promoverá un modelo de Hub Web3 democrático, constitucional, transparente, descentralizado, respetuoso de derechos fundamentales y competitivo fiscalmente.

Este modelo se diferenciará por:

a) Protección constitucional de autocustodia.
b) Identidad digital soberana.
c) Prohibición de CBDCs de control social.
d) Compliance criptográfico.
e) Regulador especializado.
f) Zona franca tecnológica.
g) Protección contra vigilancia masiva.
h) Seguridad jurídica registral blockchain.
i) Incentivos a infraestructura real.
j) Estado de Derecho y reputación democrática.

Artículo 423. Incentivos Competitivos sin Renuncia a Transparencia

Los incentivos del modelo costarricense deberán ser competitivos regionalmente, pero condicionados a cumplimiento, sustancia, auditoría, transparencia, protección de usuarios, prevención de delitos financieros y respeto a derechos fundamentales.

Artículo 424. Reconocimiento de Actividades Digitales de Exportación

Se reconocerán como actividades estratégicas de exportación los servicios digitales vinculados a blockchain, activos digitales, tokenización, IA, ciberseguridad, compliance criptográfico, desarrollo de software, auditoría, consultoría tecnológica, investigación, infraestructura y educación digital prestados desde Costa Rica hacia mercados internacionales.

SECCIÓN V — CLÁUSULAS FINALES DE SOBERANÍA FISCAL Y COMPETITIVIDAD

Artículo 425. Cláusula de No Tributación de la Soberanía Financiera Personal

Ninguna norma tributaria podrá interpretarse en el sentido de gravar la mera tenencia, autocustodia, apreciación no realizada, control de llaves privadas, transferencia entre wallets propias o posesión pasiva de Bitcoin y activos digitales descentralizados sin fuente costarricense.

Artículo 426. Cláusula de Tributación de Actividad Digital Organizada

Estarán sujetas al régimen fiscal correspondiente las actividades digitales organizadas, profesionales, empresariales o institucionales que generen renta atribuible a Costa Rica, incluyendo VASP, bolsas, bancos digitales, emisores, tokenizadores, custodios, plataformas, traders profesionales, DAOs con actividad local y servicios tecnológicos.

Artículo 427. Cláusula de Competitividad frente a Jurisdicciones Web3

La política fiscal, regulatoria y de incentivos deberá revisarse periódicamente para mantener a Costa Rica competitiva frente a jurisdicciones Web3 internacionales, incluyendo El Salvador, Suiza, Liechtenstein, Singapur, Hong Kong, Dubái, Abu Dhabi, Wyoming y otras.

La revisión deberá considerar:

a) Atracción de inversión.
b) Seguridad jurídica.
c) Costos regulatorios.
d) Tiempo de licenciamiento.
e) Incentivos fiscales.
f) Protección de derechos digitales.
g) Talento local.
h) Infraestructura tecnológica.
i) Reputación internacional.
j) Cumplimiento AML/CFT.

Artículo 428. Cláusula de Recaudación Inteligente

El Estado deberá privilegiar un modelo de recaudación inteligente basado en atracción de industria, licencias, actividad económica real, exportación de servicios, inversión tecnológica, empleo calificado, infraestructura digital y crecimiento de mercados regulados.

Se evitará un modelo de persecución fiscal sobre usuarios personales, autocustodia, tenencia pasiva o innovación no intermediada.

CAPÍTULO XV — INTENDENCIA DE LA INDUSTRIA DESCENTRALIZADA (IID) — ÓRGANO TÉCNICO DE DESCONCENTRACIÓN MÁXIMA ADSCRITO AL MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

Artículo 429. Creación de la Intendencia de la Industria Descentralizada

Créase la Intendencia de la Industria Descentralizada, en adelante IID, como órgano especializado de desconcentración máxima adscrito al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, MICITT.

La IID será la autoridad técnica especializada del Estado en materia de activos digitales, tecnologías descentralizadas, mercados digitales nativos, tokenización, infraestructura Web3, proveedores de servicios sobre activos digitales y demás materias comprendidas dentro del perímetro regulatorio establecido en esta ley.

La adscripción al MICITT no implicará subordinación jerárquica en el ejercicio de las competencias sustantivas expresamente desconcentradas por esta ley.

Artículo 430. Naturaleza Jurídica y Desconcentración Máxima

La IID será un órgano de desconcentración máxima del MICITT, dotado de independencia técnica, funcional, administrativa y de gestión presupuestaria para el ejercicio de las competencias que esta ley le atribuye.

Dentro de las materias desconcentradas, la persona titular del Ministerio, los viceministerios y demás dependencias del MICITT no podrán avocar competencias de la IID, revisar o sustituir sus decisiones, ni impartir órdenes, instrucciones o circulares sobre la forma de resolver procedimientos, licencias, clasificaciones, investigaciones, fiscalizaciones, sanciones, determinaciones de perímetro u otras actuaciones regulatorias individuales.

La IID forma parte de la Administración Central y no constituye una institución autónoma ni un ente público separado del Estado.

Para el cumplimiento de sus competencias contará con personalidad jurídica instrumental en los términos estrictamente necesarios para realizar actividad contractual, administrar los recursos presupuestarios que legalmente le correspondan y suscribir contratos o convenios de cooperación, con sujeción al ordenamiento financiero y presupuestario aplicable a los órganos desconcentrados del Gobierno Central.

Artículo 431. Relación con la Rectoría del MICITT

Corresponderá al MICITT ejercer la rectoría política nacional en las materias de ciencia, innovación, tecnología, transformación digital y aquellas otras que la legislación le atribuya.

La IID ejercerá, con independencia técnica y funcional, las competencias regulatorias, supervisoras, autorizatorias, fiscalizadoras y sancionatorias que esta ley desconcentra expresamente en su favor.

Las políticas generales del Poder Ejecutivo y del MICITT no podrán utilizarse para ordenar, condicionar o predeterminar la resolución de casos concretos sometidos a la IID.

La coordinación institucional se desarrollará sin perjuicio de la independencia técnica de la Intendencia ni de las competencias constitucionales o legales exclusivas de otras autoridades.

Artículo 432. Finalidades

La IID tendrá por finalidades otorgar seguridad jurídica a la industria digital; proteger a los usuarios y la integridad de los mercados digitales; prevenir fraude y abuso; promover competencia e innovación; aplicar un modelo de cumplimiento basado en riesgo; proteger derechos digitales; fortalecer la soberanía tecnológica; contribuir a la protección de infraestructura digital crítica en los términos de esta ley; facilitar la interoperabilidad regulatoria nacional e internacional; y prevenir la captura regulatoria, tecnológica o financiera.

Artículo 433. Independencia Técnica y Prohibición de Captura

La IID ejercerá sus competencias técnicas y regulatorias con independencia respecto de los sujetos regulados, instituciones financieras, proveedores tecnológicos, asociaciones sectoriales, organizaciones privadas y demás autoridades administrativas.

Ningún órgano del MICITT ni de otra entidad pública podrá avocarse el conocimiento de los asuntos atribuidos legalmente a la IID, sustituir su criterio técnico o revisar sus decisiones fuera de los recursos, controles y procedimientos establecidos expresamente por el ordenamiento jurídico.

Lo anterior no impedirá la coordinación interinstitucional exigida por esta ley ni la sujeción de la IID al control judicial, de legalidad, presupuestario, interno y de Hacienda Pública que corresponda.

Artículo 434. Competencia sectorial primaria

Corresponderá a la IID la regulación, autorización, registro, clasificación, supervisión y fiscalización sectorial de: a) proveedores de servicios de activos digitales; b) exchanges y plataformas de negociación de activos digitales, sean centralizados o descentralizados cuando exista control efectivo; c) custodios criptográficos; d) emisiones y ofertas de activos digitales; e) valores y instrumentos de inversión digitales nativos emitidos, registrados, negociados o liquidados de forma nativa mediante blockchain o DLT; f) tokenización y RWA; g) stablecoins y emisores privados dentro del perímetro no reservado a la autoridad monetaria; h) DAOs cuando exista actividad regulada; i) protocolos DeFi con control efectivo; j) infraestructuras de liquidación on-chain y demás actividades definidas por esta ley.

La mera utilización de blockchain para registrar o representar un instrumento financiero tradicional no trasladará por sí sola la competencia a la IID. El criterio determinante será la naturaleza digital nativa del producto, su infraestructura de emisión y negociación, y el perímetro especial definido por esta ley.

Artículo 435. Mercado digital nativo y separación respecto del mercado de valores tradicional

Los mercados digitales nativos regulados por esta ley constituyen un perímetro sectorial especializado y no quedarán sometidos a la SUGEVAL por el solo hecho de incorporar derechos de inversión, negociación secundaria o mecanismos de formación de precios, cuando el activo o instrumento se emita, registre, negocie y liquide de forma nativa bajo infraestructura digital sujeta a la IID.

La SUGEVAL conservará sus competencias sobre mercados y valores tradicionales. Los productos híbridos se resolverán mediante el procedimiento de determinación de perímetro previsto en esta ley, bajo el principio de una actividad, un regulador líder y coordinación sin duplicidad.

Artículo 436. Competencias reservadas y coordinación

La IID no sustituirá las competencias constitucionales o legales exclusivas del Banco Central de Costa Rica en política monetaria y emisión de moneda de curso legal, ni las competencias prudenciales sobre intermediación financiera bancaria, fiscalización de la Hacienda Pública, jurisdicción, investigación penal, materia electoral, telecomunicaciones u otras materias reservadas.

Cuando una actividad digital invada materialmente un perímetro reservado, la IID coordinará con la autoridad competente mediante protocolos de perímetro y supervisión conjunta, preservando un regulador líder y evitando autorizaciones duplicadas.

Artículo 437. Registro único sectorial y coordinación AML/CFT

La IID administrará el registro sectorial único de proveedores regulados por esta ley. Las obligaciones AML/CFT/FPADM derivadas de la Ley 7786 y sus reformas se cumplirán conforme al régimen especial aplicable y mediante interoperabilidad regulatoria con la SUGEF, la UIF y demás autoridades competentes.

La inscripción o licencia sectorial ante la IID no autoriza intermediación financiera bancaria ni exime obligaciones AML/CFT; de igual forma, la inscripción AML no sustituye la autorización sectorial exigida por esta ley.

Artículo 438. Potestades Regulatorias

La IID podrá emitir, dentro de la habilitación conferida por esta ley, normas técnicas, disposiciones regulatorias de carácter general, criterios, guías, circulares técnicas y actos administrativos necesarios para el ejercicio de sus competencias; conceder, suspender o revocar licencias; administrar registros; ordenar medidas correctivas; administrar sandboxes regulatorios; clasificar activos y actividades; y establecer estándares de custodia, reservas, transparencia, gobernanza y ciberseguridad.

La IID podrá requerir a los sujetos regulados los reportes regulatorios, declaraciones, certificaciones, estados, atestaciones, información operacional y demás documentación que esta ley les imponga expresamente preparar, conservar o presentar para fines de supervisión. Sus potestades de inspección se ejercerán sobre locales, sistemas, infraestructura y documentación regulatoria dentro del ámbito legal de supervisión, con proporcionalidad y debido proceso.

Las potestades de inspección de la IID no comprenderán por sí mismas la intervención de comunicaciones ni la revisión de documentos privados protegidos por el artículo 24 de la Constitución Política. El acceso a estos únicamente procederá con consentimiento válido, autorización judicial cuando corresponda o al amparo de una habilitación legal especial que cumpla los requisitos constitucionales aplicables.

Las obligaciones AML/CFT que requieran acceso a información reservada se ejercerán por las autoridades competentes conforme a la Ley N.º 7786 y demás legislación especial. Los reglamentos ejecutivos cuya emisión corresponda constitucionalmente al Poder Ejecutivo se tramitarán conforme al ordenamiento aplicable, sin alterar el contenido esencial de las competencias legalmente desconcentradas en la IID.

Artículo 439. Consejo Técnico Superior de la IID

La IID estará dirigida por un Consejo Técnico Superior integrado por cinco miembros de reconocida idoneidad e independencia profesional, con experiencia comprobada en derecho, regulación, economía digital, activos digitales, blockchain, mercados, ciberseguridad, sistemas distribuidos o materias afines.

Los miembros serán nombrados por el Consejo de Gobierno, previo concurso público de antecedentes y oposición administrado mediante un procedimiento transparente basado en mérito, idoneidad, experiencia, incompatibilidades, declaración de intereses y control de integridad. El expediente del concurso, la lista de elegibles y la motivación del nombramiento serán públicos, con las reservas legales correspondientes.

Los miembros ejercerán por seis años, con periodos escalonados y posibilidad de una única reelección. No podrán ser removidos discrecionalmente; la remoción únicamente procederá por incapacidad permanente, incumplimiento grave de deberes, incompatibilidad sobrevenida, conflicto de interés no subsanado, condena penal firme por delito doloso o falta grave declarada mediante procedimiento con debido proceso.

El Consejo sesionará válidamente con al menos cuatro miembros y adoptará sus decisiones por mayoría absoluta de los presentes, salvo los casos en que esta ley exija una mayoría superior. En caso de empate, la Presidencia ejercerá voto de calidad. Ningún miembro estará sujeto a instrucciones del jerarca ministerial respecto de decisiones regulatorias o procedimientos concretos.

Artículo 440. Intendente General de la Industria Descentralizada

El Consejo Técnico Superior nombrará, mediante concurso público de antecedentes y oposición, a la persona Intendente General de la Industria Descentralizada, responsable de la conducción técnica y ejecutiva de la IID.

La persona Intendente solo podrá ser removida por las causales objetivas establecidas en esta ley y mediante procedimiento previo que garantice debido proceso.

El cargo estará sometido a incompatibilidades, deberes de abstención, declaración de intereses, régimen de integridad y restricciones razonables anteriores y posteriores al ejercicio de la función pública.

Artículo 441. Incompatibilidades y puertas giratorias

Las autoridades y personal de alta dirección de la IID estarán sujetos a prohibiciones de conflicto de interés, deber de abstención, divulgación patrimonial y de intereses, incompatibilidades con sujetos regulados y periodos razonables de enfriamiento antes y después del cargo, conforme a la ley.

Artículo 442. Financiamiento y Gestión Presupuestaria

La IID contará con un programa presupuestario individualizado que permita identificar, administrar y fiscalizar los recursos destinados al ejercicio de sus competencias.

Su financiamiento podrá provenir de asignaciones presupuestarias, tasas regulatorias proporcionales, derechos de registro y licenciamiento, servicios técnicos autorizados por ley, cooperación nacional o internacional no condicionada y las demás fuentes legalmente permitidas.

Los ingresos, presupuestos y gastos de la IID se incorporarán al Presupuesto Nacional y se administrarán de conformidad con la Ley N.° 9524, la Ley de Administración Financiera de la República y Presupuestos Públicos y demás normativa aplicable, bajo los controles del Ministerio de Hacienda, control interno y fiscalización de la Contraloría General de la República que correspondan.

La incorporación al Presupuesto Nacional no facultará al MICITT para condicionar decisiones regulatorias individuales ni utilizar modificaciones administrativas o presupuestarias como mecanismo de interferencia en las competencias legalmente desconcentradas.

Las tasas regulatorias deberán guardar relación razonable con el costo de supervisión correspondiente y no podrán funcionar como barrera artificial de entrada ni como instrumento confiscatorio.

Artículo 443. Transparencia y rendición de cuentas

La IID publicará su presupuesto, ejecución, resoluciones de alcance general, estadísticas, criterios de clasificación, agenda regulatoria, consultas públicas, conflictos de interés declarados, indicadores de desempeño y un informe anual de riesgos y evolución del ecosistema, con las reservas estrictamente necesarias por ley.

Artículo 444. Auditoría externa e institucional

La IID estará sujeta a auditoría interna y externa, control judicial, fiscalización de la Hacienda Pública y evaluaciones periódicas de independencia, eficacia, proporcionalidad regulatoria y riesgo de captura. Sus propios sistemas críticos se someterán a estándares iguales o superiores a los exigidos al resto del sector público.

Artículo 445. Autoridad Técnica Especializada en Soberanía Digital

La IID será el órgano técnico especializado del MICITT encargado de desarrollar, aplicar, supervisar y verificar, dentro de las competencias conferidas por esta ley, los estándares técnicos mínimos de soberanía digital, resiliencia tecnológica, infraestructura descentralizada y protección de derechos digitales.

Esta competencia se ejercerá sin sustituir la rectoría política del MICITT ni las competencias constitucionales o legales exclusivas de otros poderes, órganos o instituciones.

Artículo 446. Inventario nacional de infraestructura digital crítica

La IID administrará un inventario clasificado de infraestructura digital crítica y estratégica del Estado, incluyendo sistemas que soporten identidad, registros, datos críticos, pagos, telecomunicaciones, salud, educación, justicia, servicios esenciales, nube estatal, criptografía, inteligencia artificial pública y demás sistemas cuya afectación pueda comprometer derechos, continuidad estatal, seguridad nacional o estabilidad económica.

El inventario deberá aplicar criterios de minimización y seguridad y podrá mantener información técnica reservada cuando su publicidad incremente el riesgo de ataque.

Artículo 447. Auditoría técnica de soberanía digital

Las dependencias del Poder Ejecutivo y los sujetos regulados por esta ley estarán sujetos a auditoría técnica periódica de conformidad respecto de la infraestructura digital crítica que administren o contraten. La auditoría evaluará, como mínimo, ciberseguridad, arquitectura de datos, minimización, criptografía, gestión de llaves, registro de eventos, control de accesos, dependencia de proveedores, reversibilidad, portabilidad, interoperabilidad, continuidad, resiliencia, uso de inteligencia artificial, vigilancia, cadena de suministro, software crítico, criptoagilidad y migración post-cuántica.

Respecto de poderes, órganos o instituciones con autonomía o competencias constitucionalmente exclusivas, la IID podrá realizar evaluaciones técnicas únicamente mediante mecanismos de coordinación compatibles con su autonomía y reserva funcional. Sus resultados tendrán naturaleza de hallazgos, alertas y recomendaciones, salvo que una norma constitucional o legal especial disponga expresamente otra cosa.

La auditoría técnica de la IID no constituye fiscalización financiera o presupuestaria, control jurisdiccional, dirección electoral, investigación penal ni sustitución de competencias constitucionalmente exclusivas.

Artículo 448. Estándares mínimos obligatorios

Los estándares mínimos de soberanía digital, seguridad, privacidad por diseño, interoperabilidad, reversibilidad, transparencia algorítmica y resiliencia establecidos directamente por esta ley y desarrollados técnicamente por la IID serán obligatorios para las dependencias del Poder Ejecutivo y los sujetos regulados dentro de su ámbito técnico.

En poderes, órganos e instituciones con autonomía o competencias constitucionalmente exclusivas, dichos estándares operarán como referencias técnicas de coordinación y mejores prácticas, sin perjuicio de las obligaciones que les resulten aplicables por normas constitucionales o legales específicas.

Toda contratación de infraestructura crítica del Poder Ejecutivo deberá incorporar requisitos de portabilidad, continuidad, documentación, acceso a registros, auditoría, salida ordenada y prevención de dependencia irreversible.

Artículo 449. Régimen de observaciones y remediación

Cuando la IID identifique una vulnerabilidad o incumplimiento técnico, emitirá un informe motivado con clasificación de riesgo, medidas de mitigación y plazo de remediación. Para entidades del Poder Ejecutivo y sujetos regulados, las medidas correctivas emitidas dentro de su competencia serán obligatorias y recurribles conforme a ley.

Respecto de poderes, órganos o instituciones con autonomía o competencias constitucionalmente exclusivas, la IID emitirá hallazgos técnicos, recomendaciones de remediación y alertas de riesgo, y coordinará su atención sin avocación, jerarquía ni sustitución de la competencia sustantiva. Los hallazgos de riesgo crítico deberán ser comunicados a las autoridades de control competentes conforme a la materia.

Artículo 450. Protección frente a vigilancia tecnológica estatal

La IID deberá verificar que la infraestructura pública no incorpore, sin habilitación legal suficiente, mecanismos de vigilancia masiva, scoring social, perfilamiento político generalizado, puertas traseras obligatorias, debilitamiento criptográfico, identificación universal coercitiva, interoperabilidad totalizante de datos o sistemas de IA destinados al espionaje indiscriminado de personas.

La investigación individualizada legalmente autorizada, la respuesta a incidentes y las funciones legítimas de ciberseguridad no se consideran vigilancia masiva cuando respeten necesidad, proporcionalidad, finalidad, trazabilidad y debido proceso.

Artículo 451. Sistemas de inteligencia artificial de alto impacto en el Estado

Todo sistema de inteligencia artificial de alto impacto utilizado por el sector público deberá contar, según riesgo, con evaluación previa de impacto en derechos, registro, documentación técnica, trazabilidad, pruebas de sesgo y seguridad, control humano significativo, mecanismo de impugnación y auditoría independiente.

Se prohíbe utilizar IA pública para scoring social general, persecución política, vigilancia masiva, manipulación de la ciudadanía o decisiones irrevisables que afecten derechos fundamentales.

Artículo 452. Protección de criptografía y llaves públicas críticas

La IID emitirá estándares de gestión criptográfica y de llaves para infraestructura pública crítica. Queda prohibido diseñar controles generales que obliguen a introducir puertas traseras o vulnerabilidades deliberadas en sistemas de uso general. Las excepciones investigativas deberán ser individualizadas y estar sustentadas en ley y debido proceso.

Artículo 453. Criptoagilidad y transición post-cuántica

La IID coordinará el inventario criptográfico nacional y la estrategia de criptoagilidad y migración post-cuántica, priorizando sistemas críticos, identidad, firmas, registros, comunicaciones sensibles, infraestructura financiera y llaves estatales.

Artículo 454. Licenciamiento proporcional

El régimen de licencias distinguirá entre custodia, intercambio, mercado, emisión, tokenización, stablecoins, intermediación, infraestructura y servicios técnicos. Las exigencias se graduarán según volumen, control efectivo, custodia de terceros, complejidad, riesgos operativos, protección al usuario y relevancia sistémica.

Artículo 455. Sandbox regulatorio nacional

La IID administrará un sandbox transparente, temporal y sujeto a salvaguardas para probar modelos innovadores que requieran claridad regulatoria. El ingreso al sandbox no equivaldrá a exención general de ley ni podrá reducir derechos fundamentales.

Artículo 456. Clasificación y determinación de perímetro

La IID podrá emitir resoluciones de clasificación de activos, protocolos, servicios y modelos de negocio. Las resoluciones deberán aplicar sustancia sobre forma, control efectivo, función económica, grado de descentralización y riesgo.

Cuando exista posible competencia concurrente con otra autoridad, se utilizará un procedimiento de perímetro con plazos definidos, intercambio técnico y decisión de regulador líder. La falta de acuerdo podrá someterse a los mecanismos administrativos o jurisdiccionales previstos por el ordenamiento.

Artículo 457. Mercados digitales centralizados

Los exchanges centralizados de activos digitales y las plataformas de negociación de activos o valores digitales nativos estarán sometidos a la IID, sin perjuicio de obligaciones AML/CFT y de otras competencias reservadas. La supervisión abarcará integridad de mercado, custodia, segregación, conflictos de interés, ciberseguridad, reservas, continuidad, transparencia y protección al usuario.

Artículo 458. DeFi y control efectivo

Los protocolos descentralizados sin persona o grupo con control efectivo no serán tratados automáticamente como intermediarios. Las obligaciones regulatorias seguirán la custodia, administración, control de claves, capacidad de actualización, censura, control de front-end esencial, tesorería, oráculos, comisiones discrecionales y demás indicadores de control real.

Artículo 459. Autocustodia, software libre y nodos

La IID no podrá exigir licencia por la mera tenencia de activos propios, autocustodia, desarrollo o publicación de software no custodial, operación de nodos o validadores, auditoría de código, investigación de seguridad o interacción peer-to-peer lícita. La responsabilidad deberá fundarse en conducta, control o participación efectiva en una actividad regulada o ilícita.

Artículo 460. Stablecoins y coordinación monetaria

La IID regulará emisores privados y servicios vinculados a stablecoins dentro del perímetro definido por esta ley, incluyendo reservas, redención, divulgación, gobernanza, custodia y riesgo operacional. Cuando una estructura pueda afectar política monetaria, sistemas de pago de importancia sistémica, depósitos o intermediación financiera, se coordinará con el Banco Central, SUGEF y demás autoridades competentes.

Artículo 461. Cooperación internacional y reconocimiento

La IID podrá celebrar memorandos de entendimiento, participar en redes supervisoras, intercambiar información conforme a ley y reconocer estándares o equivalencias extranjeras cuando existan niveles adecuados de supervisión y protección de derechos. La cooperación no podrá utilizarse para eludir garantías constitucionales, debido proceso o protección de datos.

Artículo 462. AML/CFT basado en riesgo

La IID colaborará con las autoridades competentes en prevención de legitimación de capitales, financiamiento del terrorismo y proliferación. El cumplimiento deberá ser basado en riesgo, proporcional y compatible con la

Recomendación 15 de GAFI, sin convertir la autocustodia, el pseudonimato legítimo o el software neutral en presunciones de ilicitud.

Artículo 463. Protección al usuario e integridad de mercado

La IID establecerá reglas de divulgación, segregación de activos, reservas, custodia, publicidad, conflictos, continuidad, manipulación de mercado, abuso de información y mecanismos de reclamo, diferenciando usuarios minoristas, profesionales e institucionales.

Artículo 464. Investigación, capacitación y observatorio tecnológico

La IID mantendrá capacidades permanentes de análisis de blockchain, smart contracts, IA, ciberseguridad, mercados digitales, neurotecnología, riesgos post-cuánticos y tecnologías emergentes. Podrá cooperar técnicamente con universidades, Poder Judicial, autoridades de investigación y organismos internacionales sin asumir funciones jurisdiccionales o penales.

Artículo 465. Revisión judicial y debido proceso

Toda licencia, sanción, orden, clasificación o medida individual de la IID deberá ser motivada, proporcional, recurrible y sujeta a control judicial. Las medidas cautelares administrativas solo procederán en los casos y con los límites expresamente definidos por ley.

Artículo 466. Evaluación regulatoria y cláusula de innovación

La IID revisará periódicamente el impacto de sus regulaciones sobre competencia, innovación, inclusión, derechos digitales y costos de cumplimiento. Deberá preferir estándares funcionales, tecnológicamente neutrales y basados en riesgo frente a prohibiciones generales cuando existan medidas menos restrictivas igualmente eficaces.

Artículo 467. Competencia Regulatoria Especializada y Armonización del Perímetro

La IID ejercerá las competencias regulatorias especializadas conferidas por esta ley, dentro del marco constitucional costarricense y bajo principios de neutralidad tecnológica, proporcionalidad, independencia técnica e interoperabilidad internacional.

Dentro de los doce meses siguientes a su instalación, la IID, en coordinación con el MICITT y las autoridades competentes, deberá identificar y proponer las reformas legales o reglamentarias necesarias para eliminar duplicidades regulatorias y armonizar los regímenes preexistentes, particularmente respecto de mercados de valores tradicionales, supervisión prudencial y registro AML/CFT de proveedores de activos virtuales.

Hasta que culmine la transición, ninguna entidad quedará exenta de obligaciones vigentes por el solo hecho de encontrarse comprendida dentro del futuro perímetro de la IID.

CAPÍTULO XVI — DAOs Y NUEVAS FORMAS DE ORGANIZACIÓN DIGITAL

SECCIÓN I — RECONOCIMIENTO JURÍDICO DE LAS DAOs

Artículo 468. Reconocimiento de las DAOs

El Estado reconoce la existencia de Organizaciones Autónomas Descentralizadas, DAOs, como formas de organización digital, coordinación colectiva, gobernanza distribuida y administración programable de recursos, protocolos, comunidades, proyectos o infraestructuras digitales.

Las DAOs podrán operar como comunidades digitales no personificadas, protocolos descentralizados con gobernanza on-chain, organizaciones registradas con personalidad jurídica, fundaciones o asociaciones digitales, entidades híbridas con wrapper legal, vehículos de tesorería descentralizada, organizaciones de gobernanza de

protocolos, organizaciones de inversión cuando la ley lo permita u organizaciones de impacto, investigación, infraestructura o desarrollo tecnológico.

La existencia técnica u operativa de una DAO no le atribuirá automáticamente personalidad jurídica costarricense. La personalidad jurídica especial prevista por esta ley nacerá únicamente con la inscripción correspondiente y el cumplimiento de los requisitos legales de constitución, domicilio, representación y responsabilidad.

Artículo 469. Definición de DAO

Para efectos de esta ley, se entenderá por DAO toda organización, comunidad, protocolo o estructura digital que coordine decisiones, recursos, reglas, tesorería, desarrollo, gobernanza o ejecución mediante smart contracts, votación digital, tokens de gobernanza, multisig, credenciales, mecanismos on-chain, reglas automatizadas o procesos descentralizados.

La existencia de una DAO no dependerá exclusivamente de tener personalidad jurídica formal, sino de su estructura funcional de coordinación digital.

Artículo 470. Naturaleza Jurídica Diferenciada

Las DAOs no serán consideradas automáticamente sociedades mercantiles, asociaciones, fideicomisos, fondos de inversión, bancos, intermediarios financieros, VASP o entidades reguladas por su sola existencia.

Su calificación dependerá de la actividad real, control efectivo, existencia de tesorería, derechos de participantes, distribución de beneficios, custodia de activos de terceros, oferta pública, gobernanza, jurisdicción, riesgos para usuarios, relación con mercados regulados y personalidad jurídica o ausencia de ella.

La responsabilidad limitada derivada de una DAO registrada o de un wrapper legal no protegerá fraude, abuso de personalidad, apropiación indebida, incumplimiento doloso, actuación personal ilícita ni ejercicio de control efectivo contrario a la ley.

SECCIÓN II — CLASIFICACIÓN DE DAOs

Artículo 471. Categorías de DAOs

La IID podrá clasificar las DAOs conforme a su función principal, incluyendo:

a) DAOs de protocolo.
b) DAOs de inversión.
c) DAOs de grants o financiamiento.
d) DAOs de infraestructura.
e) DAOs de comunidad.
f) DAOs culturales o creativas.
g) DAOs de impacto social o ambiental.
h) DAOs de RWA.
i) DAOs de tesorería.
j) DAOs de investigación.
k) DAOs de software libre.
l) DAOs de servicios profesionales.
m) DAOs híbridas.

Artículo 472. DAOs de Protocolo

Son DAOs de protocolo aquellas encargadas de gobernar, actualizar, financiar, mantener o coordinar protocolos descentralizados, smart contracts, redes, parámetros técnicos, tesorerías o infraestructura Web3.

Estas DAOs estarán sujetas a reglas proporcionales cuando ejerzan control efectivo sobre activos, liquidez, oráculos, parámetros financieros, tesorería significativa, front-ends o riesgos sistémicos.

Artículo 473. DAOs de Inversión

Son DAOs de inversión aquellas que reúnen recursos, activos digitales o aportes de participantes para realizar inversiones, adquirir activos, financiar proyectos, participar en tokenización, gestionar tesorerías o distribuir beneficios económicos.

Estas DAOs podrán requerir registro, disclosure, reglas de gobernanza, límites de participación, control AML/CFT, protección de inversionistas y régimen fiscal aplicable, según su estructura y oferta.

Artículo 474. DAOs de Software Libre, Investigación o Comunidad

Las DAOs dedicadas a software libre, investigación, educación, grants, cultura, comunidad, coordinación técnica o desarrollo abierto no estarán sujetas a licenciamiento financiero por su sola existencia, salvo que administren activos de terceros, prometan rendimientos, intermedien servicios regulados o realicen oferta pública de inversión.

SECCIÓN III — PERSONALIDAD JURÍDICA Y REGISTRO

Artículo 475. Personalidad Jurídica DAO

Las DAOs podrán adquirir personalidad jurídica en Costa Rica mediante inscripción ante el registro que determine la ley, bajo una figura especial denominada Organización Autónoma Descentralizada Registrada o DAO-CR.

La personalidad jurídica permitirá a la DAO:

a) Contratar.
b) Ser titular de derechos y obligaciones.
c) Abrir cuentas o relaciones comerciales.
d) Registrar dominios, marcas o propiedad intelectual.
e) Contratar personal o proveedores.
f) Responder limitadamente conforme a ley.
g) Acceder a regímenes de incentivos.
h) Comparecer en procesos administrativos, judiciales o arbitrales.
i) Administrar tesorerías conforme a reglas publicadas.

Artículo 476. Registro de DAOs

El Registro de DAOs deberá permitir inscripción ágil, digital, interoperable y compatible con identidad soberana, wallets, multisig, smart contracts y documentación on-chain.

La inscripción podrá requerir:

a) Nombre de la DAO.
b) Propósito.
c) Identificadores de smart contracts.
d) Dirección de tesorería o multisig.
e) Reglas de gobernanza.
f) Mecanismos de votación.
g) Representantes o signatarios legales, si los hubiere.
h) Jurisdicción de controversias.
i) Política de tesorería.
j) Régimen de responsabilidad.

k) Identificación de administradores con control efectivo, cuando existan.
l) Documento de riesgos para participantes.

Artículo 477. Wrapper Legal y Entidades Híbridas

Las DAOs podrán operar mediante wrappers legales, fundaciones, asociaciones, sociedades, fideicomisos, vehículos especiales o entidades híbridas, nacionales o extranjeras, siempre que divulguen la relación entre la entidad legal y la gobernanza on-chain.

La IID podrá reconocer wrappers extranjeros cuando cumplan estándares mínimos de transparencia, responsabilidad, AML/CFT cuando corresponda y protección de participantes.

Artículo 478. DAOs Extranjeras con Actividad en Costa Rica

Las DAOs extranjeras que realicen actividad económica significativa, oferta al público, tokenización de activos costarricenses, prestación de servicios regulados o administración de activos de terceros en Costa Rica deberán cumplir las obligaciones aplicables según su actividad.

La mera participación de residentes costarricenses en una DAO extranjera no convertirá a dicha DAO en entidad domiciliada en Costa Rica por sí sola.

SECCIÓN IV — GOBERNANZA, TESORERÍA Y RESPONSABILIDAD

Artículo 479. Gobernanza Transparente

Las DAOs registradas o que interactúen con mercados regulados deberán publicar reglas de gobernanza claras, incluyendo:

a) Requisitos de participación.
b) Derechos de voto.
c) Proceso de propuestas.
d) Quórums.
e) Mayorías.
f) Ejecución de decisiones.
g) Gestión de conflictos de interés.
h) Modificación de reglas.
i) Mecanismos de emergencia.
j) Protección de minorías cuando corresponda.

Artículo 480. Tesorerías DAO

Las tesorerías de DAOs deberán contar con mecanismos proporcionales de seguridad, transparencia, control, auditoría, segregación, autorización y rendición de cuentas.

Podrán utilizarse:

a) Multisig.
b) Timelocks.
c) Smart contracts auditados.
d) Presupuestos on-chain.
e) Reportes de gasto.
f) Votación comunitaria.
g) Controles de emergencia.
h) Auditoría externa.

i) Proof of reserves.
j) Políticas de diversificación de activos.

Artículo 481. Multisig y Control de Llaves

Cuando una DAO utilice multisig o mecanismos equivalentes para administrar tesorería, deberá establecer reglas sobre:

a) Signatarios.
b) Umbral de firmas.
c) Rotación.
d) Conflictos de interés.
e) Pérdida o compromiso de llaves.
f) Emergencias.
g) Publicidad de transacciones relevantes.
h) Responsabilidad de firmantes.
i) Auditoría.
j) Sustitución de firmantes.

Artículo 482. Responsabilidad Limitada de Participantes

Los participantes de una DAO registrada no responderán personalmente por obligaciones de la DAO por el solo hecho de votar, poseer tokens de gobernanza, participar en foros, contribuir código, proponer mejoras o interactuar con el protocolo, salvo fraude, dolo, abuso, control efectivo, actuación como administrador de hecho o responsabilidad expresamente asumida.

Artículo 483. Responsabilidad de Administradores de Hecho

Quienes ejerzan control efectivo, administración de tesorería, ejecución de decisiones, custodia de fondos, representación, promoción engañosa o dirección material de una DAO podrán responder conforme a su grado de control y conducta.

SECCIÓN V — TOKENS DE GOBERNANZA Y PARTICIPACIÓN

Artículo 484. Tokens de Gobernanza DAO

Los tokens de gobernanza podrán conferir derechos de voto, propuesta, participación, delegación, acceso, reputación o coordinación dentro de una DAO.

No serán considerados valores mobiliarios por defecto, salvo que otorguen derechos económicos, expectativa de ganancia derivada de terceros, distribución de beneficios, participación en ingresos o sean ofrecidos principalmente como inversión.

Artículo 485. Delegación de Voto y Gobernanza Delegada

Las DAOs podrán permitir delegación de voto, representantes técnicos, comités, subDAOs, councils o estructuras de gobernanza delegada, siempre que sus funciones, límites, rendición de cuentas y revocabilidad estén claramente establecidos.

Artículo 486. Protección de Minorías y Prevención de Captura

Las DAOs registradas o con relevancia económica significativa deberán adoptar mecanismos para prevenir captura por ballenas, insiders, fundadores, exchanges, custodios o actores coordinados.

Podrán establecerse:

a) Quórums reforzados.
b) Timelocks.
c) Voto cuadrático cuando sea viable.
d) Disclosure de grandes tenencias.
e) Delegación transparente.
f) Límites de conflicto de interés.
g) Mecanismos de veto técnico limitado.
h) Auditoría de concentración.
i) Gobernanza progresiva.

SECCIÓN VI — COMPLIANCE, AML/CFT Y PROTECCIÓN DE PARTICIPANTES

Artículo 487. Compliance Proporcional de DAOs

Las DAOs estarán sujetas a obligaciones de compliance únicamente cuando su actividad, estructura o control efectivo lo justifique, especialmente si:

a) Captan fondos del público.
b) Administran activos de terceros.
c) Realizan inversión colectiva.
d) Operan mercados.
e) Prestan servicios VASP.
f) Gestionan RWA.
g) Intermedian pagos.
h) Emite stablecoins.
i) Distribuyen rendimientos.
j) Tienen actividad local organizada.

Artículo 488. AML/CFT en DAOs

Las obligaciones AML/CFT aplicables a DAOs deberán implementarse de forma proporcional, basada en riesgo y compatible con privacidad, autocustodia y compliance criptográfico.

No será obligatorio identificar a todos los participantes pasivos de una DAO por el solo hecho de votar o poseer tokens, salvo que participen en actividades reguladas, administración de fondos, inversión colectiva, servicios a terceros o riesgo específico.

Artículo 489. Divulgación de Riesgos

Las DAOs que emitan tokens, reciban aportes, administren tesorerías significativas, financien proyectos o interactúen con mercados regulados deberán divulgar riesgos relevantes, incluyendo:

a) Riesgo de smart contract.
b) Riesgo de gobernanza.
c) Riesgo de concentración.
d) Riesgo de liquidez.
e) Riesgo regulatorio.
f) Riesgo de tesorería.
g) Riesgo de hacks.
h) Riesgo de oráculos.
i) Riesgo de ejecución de propuestas.
j) Riesgo de pérdida de llaves.

SECCIÓN VII — DAOs, TRIBUTACIÓN Y ACTIVIDAD ECONÓMICA

Artículo 490. Tratamiento Tributario de DAOs

El tratamiento tributario de una DAO dependerá de su personalidad jurídica, actividad económica real, residencia, fuente de ingresos, control efectivo, distribución de beneficios, tesorería, prestación de servicios y vínculo con Costa Rica.

La mera existencia de una DAO o participación de usuarios costarricenses no generará por sí sola obligación tributaria local.

Artículo 491. Distribuciones y Beneficios

Las distribuciones de beneficios, pagos, rendimientos, remuneraciones, grants, compensaciones o asignaciones patrimoniales realizadas por una DAO podrán generar efectos fiscales conforme a su naturaleza económica y jurisdicción aplicable.

No se presumirá renta personal por la mera existencia de una tesorería común no distribuida.

SECCIÓN VIII — RESOLUCIÓN DE CONTROVERSIAS Y REPRESENTACIÓN

Artículo 492. Representación Legal de DAOs

Las DAOs registradas deberán designar al menos un mecanismo de representación legal, que podrá consistir en:

a) Representante humano.
b) Comité.
c) Fundación o wrapper.
d) Multisig autorizado.
e) Agente registrado.
f) Proceso de designación on-chain.

La representación deberá permitir recibir notificaciones, comparecer ante autoridades, firmar contratos y responder frente a terceros.

Artículo 493. Resolución de Controversias DAO

Las DAOs podrán establecer mecanismos de resolución de controversias, incluyendo arbitraje digital, mediación, tribunales especializados, mecanismos on-chain, jurados descentralizados o cláusulas híbridas.

Cuando existan consumidores, inversionistas minoristas o derechos fundamentales, dichos mecanismos no podrán eliminar acceso a justicia ni garantías mínimas.

Artículo 494. Evidencia On-Chain en Controversias DAO

Las votaciones, transacciones, propuestas, smart contracts, mensajes firmados, snapshots, timelocks, ejecuciones y registros on-chain podrán utilizarse como evidencia en controversias relacionadas con DAOs.

SECCIÓN IX — DAOs PÚBLICAS, CÍVICAS Y DE IMPACTO

Artículo 495. DAOs de Impacto Público

El Estado podrá reconocer DAOs de impacto público orientadas a investigación, educación, ambiente, cultura, ciencia, innovación, transparencia, datos abiertos, infraestructura comunitaria o participación ciudadana.

Estas DAOs podrán acceder a incentivos, grants, sandboxes, colaboración institucional o regímenes especiales, siempre que respeten transparencia, rendición de cuentas y derechos fundamentales.

Artículo 496. Prohibición de DAOs para Captura de Funciones Públicas

Las DAOs no podrán sustituir funciones públicas esenciales, ejercer potestades de imperio, administrar derechos fundamentales, decidir beneficios públicos o gestionar procesos electorales sin habilitación legal expresa, garantías constitucionales y supervisión institucional.

SECCIÓN X — CLÁUSULAS FINALES SOBRE DAOs

Artículo 497. Cláusula Pro Innovación Organizacional

Toda interpretación sobre DAOs deberá favorecer la innovación organizacional, coordinación descentralizada, software libre, participación comunitaria, autonomía privada, transparencia on-chain y protección de participantes, siempre dentro del marco de legalidad y prevención de abuso.

Artículo 498. Cláusula Anti Simulación DAO

Será contrario a esta ley utilizar la apariencia de DAO para ocultar una empresa centralizada, evadir responsabilidad, defraudar inversionistas, captar fondos ilícitamente, manipular mercados, evitar AML/CFT aplicable o transferir riesgos a participantes sin disclosure.

Artículo 499. Cláusula de Reconocimiento Evolutivo

La IID podrá emitir guías, categorías, criterios y estándares para nuevas formas de organización digital que evolucionen más allá de las DAOs, siempre bajo consulta pública, neutralidad tecnológica, proporcionalidad, protección de derechos y respeto a descentralización efectiva.

CAPÍTULO XVII — MINERÍA DIGITAL, VALIDADORES, NODOS, INFRAESTRUCTURA COMPUTACIONAL DESCENTRALIZADA Y SOBERANÍA ENERGÉTICA DIGITAL

SECCIÓN I — PRINCIPIOS FUNDAMENTALES

Artículo 500. Reconocimiento de Infraestructura Descentralizada

El Estado reconoce como infraestructura descentralizada lícita la operación de sistemas, equipos, redes, software, nodos, validadores, mineros, oráculos, relayers, indexadores, secuenciadores, almacenamiento distribuido, computación descentralizada y demás componentes técnicos que permitan operar redes blockchain, protocolos Web3/Web4 y sistemas criptográficos.

Dicha infraestructura podrá ser desarrollada, operada, auditada, mantenida y utilizada por personas físicas, jurídicas, DAOs, universidades, empresas, comunidades técnicas, instituciones públicas o privadas, conforme a la ley.

Artículo 501. Neutralidad Tecnológica de Infraestructura

La operación de infraestructura descentralizada no será considerada por sí sola actividad financiera, intermediación, custodia, emisión de activos digitales, captación pública, transmisión de dinero, VASP, banco, bolsa, fiduciario o proveedor de inversión.

La calificación jurídica dependerá de la actividad concreta, existencia de custodia, prestación profesional de servicios a terceros, control efectivo sobre activos, intermediación económica o actividad regulada adicional.

Artículo 502. Protección Legal de Infraestructura Descentralizada

El Estado no podrá prohibir, restringir, discriminar o criminalizar de forma general la operación lícita de infraestructura descentralizada por su naturaleza tecnológica, criptográfica, peer-to-peer, global, pseudónima o resistente a censura.

Toda limitación deberá ser legal, proporcional, motivada, técnicamente justificada y orientada a riesgos concretos.

SECCIÓN II — MINERÍA DIGITAL

Artículo 503. Reconocimiento de la Minería Digital

Se reconoce la minería digital como actividad tecnológica lícita mediante la cual se aportan recursos computacionales, energéticos y criptográficos para asegurar redes blockchain, validar transacciones, mantener consenso, emitir recompensas de protocolo y proteger sistemas descentralizados.

La minería digital podrá realizarse de forma individual, comunitaria, empresarial, académica, industrial o institucional, conforme a las normas ambientales, energéticas, tributarias, municipales y de seguridad aplicables.

Artículo 504. Minería como Actividad Tecnológica Lícita

La minería digital no será considerada por sí sola actividad financiera regulada, VASP, custodia, intermediación, emisión privada, captación pública o prestación de servicios financieros.

Podrá considerarse actividad económica, industrial o tecnológica cuando se realice de forma habitual, organizada, comercial o empresarial desde territorio costarricense.

Artículo 505. Energía y Minería Sostenible

La minería digital deberá realizarse conforme a principios de eficiencia energética, sostenibilidad, cumplimiento ambiental, uso responsable de recursos, transparencia operativa y respeto a la infraestructura eléctrica nacional.

El Estado podrá promover minería vinculada a:

a) Energías renovables.
b) Excedentes energéticos.
c) Energía desperdiciada o no despachable.
d) Microredes.
e) Proyectos de estabilización energética.
f) Aprovechamiento de energía geotérmica, hidroeléctrica, solar, eólica o biomasa.
g) Innovación en eficiencia térmica y reutilización de calor.

Artículo 506. Incentivos para Minería Estratégica

El Estado podrá establecer incentivos para proyectos de minería digital que contribuyan a:

a) Uso de energía renovable.
b) Estabilización de redes eléctricas.
c) Inversión en infraestructura energética.
d) Desarrollo regional.
e) Investigación en eficiencia computacional.
f) Generación de empleo técnico.
g) Exportación de servicios digitales.
h) Seguridad de redes descentralizadas.
i) Aprovechamiento de excedentes energéticos.
j) Desarrollo de centros de datos especializados.

SECCIÓN III — VALIDADORES, NODOS Y PARTICIPACIÓN EN REDES

Artículo 507. Reconocimiento de Validadores

Se reconoce la función de validadores en redes blockchain, proof-of-stake, proof-of-authority, proof-of-history, rollups, capas de liquidación, redes de disponibilidad de datos y demás sistemas de consenso o verificación.

Los validadores podrán operar infraestructura, proponer bloques, verificar transacciones, participar en consenso, recibir recompensas, ejecutar software de red, delegar o recibir delegaciones, conforme a las reglas del protocolo y la ley aplicable.

Artículo 508. Operación de Nodos

Toda persona podrá operar nodos completos, nodos ligeros, nodos archivísticos, nodos validadores, nodos RPC, nodos de indexación, nodos de almacenamiento, nodos de disponibilidad de datos o nodos de verificación en redes descentralizadas lícitas.

La operación de nodos no requerirá licencia financiera por sí misma, salvo que se presten servicios adicionales regulados, custodia de terceros, intermediación o actividad económica sometida a autorización.

Artículo 509. Nodos Personales y Autocustodia

El Estado protegerá el derecho de las personas a operar nodos personales para verificar transacciones, interactuar con wallets, proteger privacidad, evitar dependencia de terceros, fortalecer autocustodia y participar en redes descentralizadas.

Ninguna autoridad podrá exigir que los usuarios dependan exclusivamente de nodos, RPC, custodios o proveedores autorizados para interactuar con redes públicas lícitas.

Artículo 510. Neutralidad sobre Software y Protocolos

La instalación, ejecución, compilación, auditoría, modificación, publicación o distribución de software de nodos, validadores, clientes blockchain, wallets, herramientas de minería o infraestructura descentralizada no constituirá por sí sola actividad regulada.

La responsabilidad jurídica surgirá por uso ilícito, fraude, control de activos de terceros, explotación maliciosa, intermediación regulada o incumplimiento de obligaciones específicas.

SECCIÓN IV — INFRAESTRUCTURA DESCENTRALIZADA AVANZADA

Artículo 511. Infraestructura de Pruebas de Conocimiento Cero

Se reconoce la infraestructura de pruebas de conocimiento cero, generación de pruebas, verificadores, circuitos, rollups, zkVMs, zkEVMs, sistemas de privacidad, identidad selectiva y compliance criptográfico como infraestructura estratégica para privacidad, escalabilidad, cumplimiento proporcional y soberanía digital.

El Estado promoverá su investigación, adopción y uso en identidad digital, compliance, mercados, Registro Público, elecciones, privacidad financiera y protección de datos.

Artículo 512. Infraestructura Post-Cuántica

Se reconoce la infraestructura de criptografía post-cuántica, criptoagilidad, migración de llaves, firmas resistentes a ataques cuánticos y mecanismos híbridos como infraestructura crítica para la continuidad de redes, identidad, registros, mercados y sistemas públicos.

La IID, junto con autoridades competentes, promoverá estándares, pilotos, investigación y planes de migración post-cuántica para infraestructura Web3 crítica.

Artículo 513. Infraestructura de IA Descentralizada

Se reconoce la infraestructura de inteligencia artificial descentralizada, federada, distribuida, verificable y privada por diseño como componente estratégico de soberanía algorítmica.

Podrá incluir:

a) Redes de cómputo distribuido.
b) Entrenamiento federado.
c) Modelos auditables.
d) Mercados de GPU.
e) Verificación de inferencia.
f) Proof of compute.
g) Modelos open-source.
h) Infraestructura de datos soberanos.
i) Sistemas de IA interoperables con blockchain.

Artículo 514. Decentralized Cloud y Compute

El Estado reconocerá y promoverá infraestructuras de almacenamiento descentralizado, decentralized cloud, edge computing, compute marketplaces, redes de contenido descentralizadas, servidores soberanos y sistemas distribuidos como alternativas legítimas a infraestructuras centralizadas.

Estas infraestructuras podrán ser utilizadas para servicios públicos, privados, académicos o comunitarios cuando cumplan estándares de seguridad, privacidad, resiliencia y disponibilidad.

SECCIÓN V — ENERGÍA, CENTROS DE DATOS Y SOBERANÍA TECNOLÓGICA

Artículo 515. Centros de Datos Web3

Los centros de datos Web3, blockchain, IA, validación, minería, ZKP, post-cuántica, decentralized cloud o infraestructura digital avanzada serán reconocidos como infraestructura tecnológica estratégica.

Su desarrollo podrá acogerse a incentivos, permisos ágiles, estándares de eficiencia, seguridad física, ciberseguridad, energía renovable y sostenibilidad.

Artículo 516. Incentivos Energéticos

El Estado podrá establecer incentivos para proyectos de infraestructura computacional que:

a) Utilicen energía renovable.
b) Compren excedentes eléctricos.
c) Inviertan en generación limpia.
d) Estabilicen demanda.
e) Generen empleo técnico.
f) Se ubiquen en zonas de menor desarrollo.
g) Aporten a resiliencia energética.
h) Implementen eficiencia térmica.
i) Reutilicen calor.
j) Integren almacenamiento energético.

Artículo 517. Redes Distribuidas y Mesh Networks

Se reconoce el valor estratégico de redes distribuidas, mesh networks, redes comunitarias, redes resilientes, sistemas alternativos de conectividad y comunicaciones descentralizadas para continuidad operativa, respuesta a emergencias, inclusión digital y soberanía tecnológica.

Su desarrollo deberá respetar normativa de telecomunicaciones, seguridad, privacidad, espectro y derechos fundamentales.

Artículo 518. Protección de Infraestructura Crítica Descentralizada

La infraestructura descentralizada que soporte mercados digitales, identidad soberana, Registro Público blockchain, sistemas electorales, banca digital, redes de pagos, ciberseguridad, IA o servicios esenciales podrá ser declarada infraestructura crítica digital.

Dicha declaratoria no podrá utilizarse para capturar, centralizar o controlar indebidamente la infraestructura descentralizada.

SECCIÓN VI — SUPERVISIÓN Y LÍMITES REGULATORIOS

Artículo 519. Infraestructura Neutral No Financiera

La infraestructura neutral no financiera comprenderá la operación de nodos, validadores, mineros, servidores, relayers, oráculos, indexadores, clientes de software, almacenamiento descentralizado y otros sistemas técnicos que no custodien, intermedien ni administren activos de terceros.

Dicha infraestructura no estará sujeta a licencias financieras por su sola operación.

Artículo 520. Límites a la Regulación de Infraestructura

Toda regulación sobre minería, nodos, validadores, centros de datos, infraestructura descentralizada o computación distribuida deberá basarse en riesgos concretos: energía, ambiente, ciberseguridad, protección de consumidores, AML/CFT cuando exista intermediación, competencia, seguridad física o infraestructura crítica.

No podrán imponerse requisitos que, por su costo o complejidad, equivalgan a una prohibición indirecta de operación descentralizada lícita.

Artículo 521. Prohibición de Criminalización Tecnológica

Queda prohibido criminalizar, sancionar o presumir ilicitud por:

a) Operar un nodo.
b) Minar activos digitales.
c) Validar transacciones.
d) Ejecutar software blockchain.
e) Usar hardware especializado.
f) Participar en consenso.
g) Hospedar infraestructura descentralizada.
h) Ejecutar un relay o indexador.
i) Proveer almacenamiento distribuido.
j) Desarrollar infraestructura open-source.

La responsabilidad surgirá por conductas ilícitas específicas, no por la herramienta tecnológica utilizada.

SECCIÓN VII — INNOVACIÓN Y COMPETITIVIDAD NACIONAL

Artículo 522. Incentivos a Infraestructura Estratégica

El Estado podrá incentivar inversión nacional e internacional en infraestructura computacional descentralizada, centros de datos, minería sostenible, validadores institucionales, infraestructura ZKP, post-cuántica, decentralized cloud, IA distribuida, seguridad blockchain y nodos públicos.

Estos incentivos podrán integrarse al Régimen Especial de Zona Franca Tecnológica y Digital.

Artículo 523. Investigación y Desarrollo

El Estado promoverá investigación en:

a) Minería eficiente.
b) Consenso descentralizado.
c) Seguridad de validadores.
d) ZKP.
e) Criptografía post-cuántica.
f) Computación distribuida.
g) IA descentralizada.
h) Redes peer-to-peer.
i) Seguridad de oráculos.
j) Infraestructura de rollups.
k) Ciberseguridad Web3.

Artículo 524. Soberanía Computacional

Costa Rica reconocerá la soberanía computacional como la capacidad nacional de acceder, operar, auditar, desplegar y proteger infraestructura de cómputo crítica para blockchain, IA, ciberseguridad, identidad, mercados digitales, registros públicos y servicios esenciales.

La política pública deberá promover diversidad de proveedores, capacidad local, interoperabilidad, formación técnica, energía sostenible y resiliencia.

SECCIÓN VIII — CLÁUSULAS FINALES

Artículo 525. Cláusula Anti Monopolio Tecnológico

El Estado deberá evitar que la infraestructura computacional descentralizada quede capturada por monopolios de nube, energía, telecomunicaciones, hardware, validación, minería, nodos, RPC, oráculos o proveedores críticos.

Artículo 526. Cláusula de Infraestructura Libre

Toda norma relativa a infraestructura Web3 deberá interpretarse a favor de la operación lícita, interoperable, segura, descentralizada y competitiva de redes, nodos, validadores, minería, cómputo distribuido y software abierto.

Artículo 527. Cláusula de Resiliencia Digital Nacional

La infraestructura descentralizada será considerada parte de la resiliencia digital nacional cuando contribuya a continuidad, verificación, privacidad, seguridad, soberanía tecnológica, mercados abiertos, identidad soberana, ciberseguridad o resistencia a censura.

SECCIÓN IX — SOBERANÍA ENERGÉTICA DIGITAL, INFRAESTRUCTURA COMPUTACIONAL Y REDES DESCENTRALIZADAS

Artículo 528. Principio de Soberanía Energética Digital

El Estado reconocerá que la infraestructura digital avanzada, incluyendo inteligencia artificial, blockchain, minería digital, validadores, data centers, computación cuántica, infraestructura post-cuántica, cloud soberano y sistemas descentralizados, depende estructuralmente de disponibilidad energética segura, renovable, competitiva y resiliente. La política energética nacional deberá contemplar la dimensión digital de la soberanía tecnológica, promoviendo capacidad eléctrica suficiente, innovación renovable, eficiencia, resiliencia, descentralización y

aprovechamiento estratégico de ventajas nacionales.

Artículo 529. Prioridad Renovable para Infraestructura Digital Estratégica

La instalación y operación de centros de datos, minería digital, validadores, infraestructura IA, nodos, servicios cloud, laboratorios computacionales y otras cargas digitales intensivas deberá priorizar fuentes renovables, eficiencia energética, gestión responsable de demanda, estándares ambientales y trazabilidad de consumo. Costa Rica podrá crear incentivos para infraestructura digital alimentada por energía renovable, excedentes, energía limpia verificable o soluciones de eficiencia que fortalezcan la competitividad tecnológica nacional sin comprometer seguridad energética ni tarifas esenciales.

Artículo 530. Minería Digital como Estabilizador Energético

La minería digital y otras cargas computacionales flexibles podrán reconocerse como herramientas potenciales de estabilización energética cuando puedan absorber excedentes, reducir desperdicio, financiar infraestructura renovable, operar bajo esquemas de respuesta a la demanda, desconectarse en picos críticos o ubicarse cerca de fuentes subutilizadas. La autoridad competente podrá autorizar modelos piloto con criterios de eficiencia, transparencia, medición, impacto tarifario, sostenibilidad, seguridad de red y beneficio nacional.

Artículo 531. Microgrids, Energía Distribuida y Resiliencia Digital

El Estado promoverá microgrids, generación distribuida, almacenamiento energético, comunidades energéticas, medición inteligente, infraestructura resiliente y redes locales capaces de sostener nodos, validadores, telecomunicaciones críticas, servicios públicos digitales, sistemas electorales, registros, salud, justicia y ciberseguridad durante fallas, emergencias o ataques. Estas infraestructuras deberán diseñarse con estándares de seguridad, interoperabilidad, resiliencia climática y continuidad operativa.

Artículo 532. Tokenización Energética y Mercados Digitales de Energía

Podrán desarrollarse modelos de tokenización energética para representar certificados de energía renovable, créditos energéticos, contratos de suministro, trazabilidad de consumo, financiamiento de infraestructura, participación en proyectos renovables, almacenamiento, flexibilidad de demanda, microgrids y otros activos o derechos energéticos permitidos por ley.

La IID regulará exclusivamente la capa digital, tokenizada o de infraestructura descentralizada comprendida en su competencia. Nada de este capítulo modifica las atribuciones de las autoridades del sector energético ni los requisitos ambientales, tarifarios, concesionales, municipales o relativos al dominio público establecidos por el ordenamiento.

La tokenización energética deberá respetar regulación sectorial, protección al consumidor, trazabilidad real, prevención de doble conteo, auditoría, sostenibilidad, transparencia y seguridad jurídica.

Artículo 533. Eficiencia Energética de Infraestructura Computacional

Los operadores de infraestructura computacional intensiva deberán adoptar medidas razonables de eficiencia energética, gestión térmica, aprovechamiento de calor residual cuando sea viable, monitoreo de consumo, estándares técnicos, mitigación ambiental y reportes proporcionales conforme al riesgo, escala e impacto. La regulación deberá evitar cargas desproporcionadas a operadores pequeños, nodos domésticos, validadores comunitarios o infraestructura descentralizada de bajo impacto.

Artículo 534. Infraestructura Energética para IA, Cloud y Computación Cuántica

La planificación nacional deberá considerar la demanda energética futura asociada a inteligencia artificial, cloud soberano, ciberseguridad, computación cuántica, laboratorios post-cuánticos, data centers, almacenamiento distribuido, simulación científica y plataformas Web3/Web4. El Estado podrá promover zonas de infraestructura digital energética, alianzas público-privadas, incentivos de inversión, educación técnica y marcos de sostenibilidad para atraer operaciones de alto valor agregado compatibles con la matriz energética nacional.

Artículo 535. Protección de Infraestructura Energética Digital como Infraestructura Crítica

La infraestructura energética que soporte servicios digitales críticos, redes blockchain públicas de relevancia nacional, sistemas electorales, registros públicos, cloud soberano, salud, pagos, ciberseguridad, telecomunicaciones y servicios esenciales será considerada infraestructura crítica cuando su interrupción pueda afectar derechos fundamentales, seguridad nacional o continuidad institucional. Deberá contar con planes de ciberseguridad, resiliencia física, redundancia, respuesta a incidentes y coordinación interinstitucional.

Artículo 536. No Criminalización del Consumo Computacional Lícito

El consumo energético asociado a minería, validadores, nodos, IA, data centers o infraestructura computacional lícita no podrá ser criminalizado por su naturaleza tecnológica. La regulación deberá enfocarse en eficiencia, legalidad, seguridad de red, sostenibilidad, impacto tarifario y cumplimiento ambiental, sin discriminación tecnológica arbitraria.

CAPÍTULO XVIII — PROTECCIÓN DEL USUARIO, CONSUMIDOR DIGITAL, INTEGRIDAD DE MERCADO Y PUBLICIDAD WEB3

SECCIÓN I — PRINCIPIOS DE PROTECCIÓN DEL USUARIO DIGITAL

Artículo 537. Derecho a Información Clara, Veraz y Comprensible

Toda persona usuaria de servicios relacionados con activos digitales tendrá derecho a recibir información clara, veraz, suficiente, accesible y comprensible sobre la naturaleza del producto, servicio, activo digital, plataforma, protocolo, token, stablecoin, RWA, smart contract o mecanismo de inversión ofrecido.

La información deberá permitir comprender, al menos:

a) Naturaleza del activo o servicio.
b) Riesgos principales.
c) Existencia o inexistencia de emisor.
d) Custodia o autocustodia.
e) Derechos conferidos.
f) Comisiones.
g) Liquidez.
h) Volatilidad.
i) Riesgos tecnológicos.
j) Riesgos regulatorios.
k) Posibles conflictos de interés.
l) Mecanismos de reclamo.

Artículo 538. Protección contra Fraude Digital

Queda prohibida toda práctica destinada a inducir a error, ocultar riesgos, falsear información, simular respaldo, prometer rendimientos inexistentes, manipular precios, fabricar liquidez, ocultar conflictos de interés, apropiarse de fondos de usuarios o presentar como descentralizado un sistema que conserva control centralizado relevante.

La IID deberá coordinar con autoridades competentes para prevenir, investigar y sancionar fraudes vinculados a activos digitales, sin criminalizar tecnologías neutrales, autocustodia, DeFi legítimo o software abierto.

Artículo 539. Prohibición de Paternalismo Regulatorio

La protección del usuario no podrá utilizarse como justificación para prohibir la autocustodia, eliminar la libertad financiera, impedir acceso a DeFi, bloquear Bitcoin, restringir software no custodial o imponer intermediación obligatoria universal.

El usuario tendrá derecho a asumir riesgos lícitos, siempre que no medie engaño, manipulación, fraude, abuso de posición dominante o incumplimiento de deberes de información por parte de sujetos regulados.

Artículo 540. Educación Financiera Digital

La IID, en coordinación con instituciones educativas, sector privado, comunidades técnicas y sociedad civil, promoverá programas de educación financiera digital sobre:

a) Bitcoin.
b) Activos digitales.
c) Autocustodia.
d) Seguridad de llaves privadas.
e) Fraudes frecuentes.
f) Phishing.
g) Smart contracts.
h) DeFi.
i) Stablecoins.
j) RWA.
k) Riesgos de volatilidad.
l) Protección de datos.
m) Compliance criptográfico.
n) Publicidad engañosa.

SECCIÓN II — DISCLOSURE Y DEBERES DE INFORMACIÓN

Artículo 541. Documento de Riesgos para Ofertas al Público

Toda oferta pública, promoción masiva o comercialización organizada de activos digitales deberá contar con un documento de riesgos proporcional al producto o servicio ofrecido.

Dicho documento deberá explicar:

a) Naturaleza del activo.
b) Función económica.
c) Derechos del adquirente.
d) Riesgos técnicos.
e) Riesgos financieros.
f) Riesgos de liquidez.
g) Riesgos de pérdida total.
h) Existencia de custodio o autocustodia.

i) Dependencia de terceros.
j) Riesgos de smart contracts.
k) Riesgos de gobernanza.
l) Riesgos regulatorios.
m) Comisiones.
n) Conflictos de interés.

Artículo 542. Riesgos Obligatorios en Activos Digitales

La IID podrá establecer advertencias mínimas obligatorias según tipo de activo digital, incluyendo:

a) Riesgo de volatilidad.
b) Riesgo de pérdida total.
c) Riesgo tecnológico.
d) Riesgo de custodia.
e) Riesgo de hackeo.
f) Riesgo de iliquidez.
g) Riesgo de depeg en stablecoins.
h) Riesgo de rug pull.
i) Riesgo de concentración.
j) Riesgo de gobernanza.
k) Riesgo de contraparte.
l) Riesgo de regulación futura.

Artículo 543. Riesgos en DeFi, Smart Contracts y Stablecoins

Cuando se ofrezcan productos o accesos relacionados con DeFi, smart contracts o stablecoins, deberá advertirse de forma especial sobre:

a) Riesgo de código.
b) Riesgo de exploits.
c) Riesgo de oráculos.
d) Riesgo de liquidaciones automáticas.
e) Riesgo de impermanent loss.
f) Riesgo de admin keys.
g) Riesgo de cambios de protocolo.
h) Riesgo de gobernanza.
i) Riesgo de depeg.
j) Riesgo de reservas insuficientes.
k) Riesgo de bridges.
l) Riesgo de slashing.

Artículo 544. Riesgos de Autocustodia

Toda plataforma, banco digital, VASP, programa educativo o proveedor que facilite autocustodia deberá informar al usuario sobre:

a) Pérdida de llaves privadas.
b) Phishing.
c) Malware.
d) Firmas maliciosas.
e) Contratos falsos.
f) Recuperación limitada.

g) Seguridad de hardware wallets.
h) Multisig.
i) Backups.
j) Protección de seed phrases.
k) Riesgos de delegación de acceso.

Estas advertencias no podrán utilizarse para desincentivar indebidamente la autocustodia ni imponer custodia obligatoria.

SECCIÓN III — PUBLICIDAD, INFLUENCERS Y PROMOCIÓN WEB3

Artículo 545. Publicidad Veraz y No Engañosa

Toda publicidad, promoción, recomendación comercial, campaña digital o comunicación pública sobre activos digitales deberá ser veraz, equilibrada, identificable como publicidad cuando corresponda y no inducir a error.

Queda prohibida la publicidad que:

a) Oculte riesgos relevantes.
b) Prometa rendimientos garantizados sin base real.
c) Simule respaldo estatal inexistente.
d) Use lenguaje bancario engañoso.
e) Presente activos de alto riesgo como seguros.
f) Exagere liquidez.
g) Oculte comisiones.
h) Omita conflictos de interés.
i) Use testimonios falsos.
j) Manipule urgencia o miedo de perder oportunidad.

Artículo 546. Prohibición de Promesas Garantizadas

Queda prohibido ofrecer, publicitar o insinuar rendimientos garantizados, ingresos pasivos seguros, rentabilidad fija, ausencia de riesgo o protección de capital en activos digitales, salvo que exista respaldo jurídico, financiero y regulatorio suficiente y se divulgue claramente la entidad responsable.

Artículo 547. Influencers, Embajadores y Promotores

Toda persona que promocione activos digitales, tokens, plataformas, protocolos, NFTs financieros, stablecoins, RWA, proyectos DeFi o servicios Web3 a cambio de pago, comisión, token allocation, beneficio económico, referral, participación o ventaja deberá divulgar de forma clara dicha relación.

Los influencers, embajadores, asesores comerciales y promotores responderán cuando participen conscientemente en publicidad engañosa, ocultamiento de compensación, manipulación de mercado, promoción de fraude o promesas falsas de rendimiento.

Artículo 548. Conflictos de Interés en Promoción

Los emisores, plataformas, market makers, asesores, influencers, founders, insiders y promotores deberán divulgar conflictos de interés materiales, incluyendo:

a) Tenencia significativa del token.
b) Lockups.
c) Vesting.
d) Compensaciones.
e) Comisiones de referral.

f) Participación en market making.
g) Relación con exchanges.
h) Control de liquidez.
i) Capacidad de venta anticipada.
j) Acceso a información privilegiada.

SECCIÓN IV — INTEGRIDAD DE MERCADO

Artículo 549. Prohibición de Manipulación de Mercado

Queda prohibida toda práctica destinada a manipular artificialmente precio, volumen, liquidez, demanda, oferta, percepción de mercado, reputación o disponibilidad de activos digitales.

Se consideran prácticas prohibidas, entre otras:

a) Wash trading.
b) Spoofing.
c) Pump and dump.
d) Front-running abusivo.
e) Manipulación de oráculos.
f) Falsa liquidez.
g) Coordinación engañosa.
h) Rumores falsos intencionales.
i) Operaciones simuladas.
j) Uso de información privilegiada.
k) Manipulación de gobernanza para beneficio oculto.

Artículo 550. Rug Pulls y Abandono Fraudulento

Se prohíben los rug pulls, entendidos como esquemas en los cuales promotores, administradores, insiders o personas con control efectivo retiran liquidez, abandonan proyectos, modifican reglas, drenan tesorerías o capturan fondos de usuarios mediante engaño, ocultamiento o abuso de confianza.

No constituirá rug pull el fracaso comercial, técnico o comunitario de un proyecto cuando haya existido divulgación adecuada de riesgos, ausencia de dolo y manejo transparente de recursos.

Artículo 551. Insider Trading Digital

Queda prohibido utilizar información material no pública para obtener ventaja indebida en la compra, venta, listado, delisting, emisión, modificación, gobernanza o negociación de activos digitales en mercados regulados o de relevancia pública.

Se considerará información material no pública, entre otras:

a) Próximos listados.
b) Hacks no divulgados.
c) Cambios de reservas.
d) Modificaciones de smart contracts.
e) Delistings.
f) Acuerdos institucionales.
g) Cambios regulatorios conocidos anticipadamente.
h) Vulnerabilidades críticas.
i) Decisiones de tesorería DAO relevantes.
j) Cambios de tokenomics.

Artículo 552. Wash Trading, Spoofing y Pump and Dump

La IID deberá establecer reglas específicas para detectar, prevenir y sancionar wash trading, spoofing, pump and dump, operaciones simuladas, volumen falso, manipulación de liquidez, bots manipulativos y coordinación artificial de precios.

Las reglas deberán distinguir entre manipulación dolosa, actividad algorítmica legítima, market making transparente, volatilidad natural y experimentación descentralizada no fraudulenta.

Artículo 553. Manipulación de Oráculos, Bridges y Parámetros Críticos

Queda prohibida la manipulación dolosa de oráculos, bridges, mecanismos de precios, datos externos, liquidaciones, validadores, gobernanza, parámetros de riesgo o sistemas de actualización con el fin de obtener beneficio indebido o causar perjuicio a usuarios o mercados.

SECCIÓN V — SEGURIDAD DEL USUARIO Y DEBERES DE PLATAFORMAS

Artículo 554. Ciberseguridad Mínima de Plataformas Reguladas

Las plataformas reguladas deberán implementar controles proporcionales de ciberseguridad, incluyendo:

a) Protección de cuentas.
b) Autenticación fuerte.
c) Gestión de llaves.
d) Auditoría de smart contracts.
e) Monitoreo de incidentes.
f) Pruebas de penetración.
g) Planes de continuidad.
h) Protección contra phishing.
i) Seguridad de APIs.
j) Gestión de vulnerabilidades.
k) Reporte de incidentes.
l) Segregación de ambientes críticos.

Artículo 555. Custodia y Segregación de Activos

Los custodios, exchanges, bancos digitales y plataformas que administren activos de terceros deberán mantener segregación patrimonial entre activos propios y activos de clientes.

No podrán prestar, pignorar, invertir, reutilizar o disponer de activos de usuarios sin autorización expresa, específica e informada.

Deberán implementar proof of reserves, controles de llaves, auditorías externas y políticas claras ante insolvencia.

Artículo 556. Reporte de Incidentes

Las plataformas reguladas deberán reportar incidentes relevantes de seguridad, pérdida de fondos, hackeos, exploits, fallas críticas, exposición de datos, insolvencia técnica, depeg significativo, manipulación de mercado o vulnerabilidades materiales.

El reporte deberá realizarse a la IID y, cuando corresponda, a usuarios afectados, sin retrasos injustificados.

Artículo 557. Mecanismos de Reclamo y Atención al Usuario

Los sujetos regulados deberán contar con mecanismos claros, accesibles y documentados para recibir, tramitar y resolver reclamos de usuarios.

Estos mecanismos deberán incluir:

a) Canal de contacto.
b) Plazos razonables.
c) Registro de reclamos.
d) Respuesta motivada.
e) Escalamiento.
f) Protección frente a bloqueos arbitrarios.
g) Procedimientos para incidentes de seguridad.
h) Información sobre recursos disponibles.

SECCIÓN VI — PROTECCIÓN ESPECIAL SIN DESTRUIR AUTOCUSTODIA

Artículo 558. Usuarios Principiantes y Advertencias Reforzadas

Cuando plataformas o proveedores regulados ofrezcan servicios a usuarios principiantes, deberán implementar advertencias reforzadas, lenguaje claro, herramientas educativas y mecanismos de confirmación de comprensión para productos de alto riesgo.

Esto no implicará prohibición de acceso, salvo casos definidos por ley para productos complejos, apalancados o de riesgo extremo.

Artículo 559. Deberes de Advertencia en Productos Complejos

Los productos complejos, apalancados, derivados, DeFi de alto riesgo, yield products, staking-as-a-service, tokens sintéticos, productos estructurados y RWA complejos deberán incluir advertencias específicas y evaluación proporcional de idoneidad cuando sean ofrecidos al público minorista.

Artículo 560. No Criminalización del Riesgo Voluntario

La pérdida económica derivada de volatilidad, caída de precio, fallas no dolosas, riesgo asumido, liquidación automática, impermanent loss o decisión informada del usuario no generará por sí sola responsabilidad administrativa, civil o penal.

La responsabilidad surgirá cuando exista fraude, engaño, negligencia grave, ocultamiento de información, manipulación, incumplimiento de deberes o abuso.

Artículo 561. Cláusula de Libertad Responsable

Toda protección al usuario deberá interpretarse conforme al equilibrio entre libertad financiera, derecho a asumir riesgos, información clara, prevención de fraude, autocustodia, innovación abierta y responsabilidad individual.

Será contrario a esta ley utilizar la protección al usuario como pretexto para eliminar opciones libres, imponer custodios obligatorios, prohibir DeFi legítimo o bloquear acceso a redes descentralizadas.

SECCIÓN VII — FRAUDES DIGITALES ESPECÍFICOS Y CONDUCTAS PROHIBIDAS

Artículo 562. Phishing, Suplantación y Estafas Web3

Queda prohibido utilizar interfaces falsas, dominios engañosos, firmas maliciosas, suplantación de plataformas, contratos falsificados, mensajes fraudulentos, deepfakes, bots o cualquier mecanismo destinado a obtener llaves privadas, seed phrases, firmas, credenciales, fondos o accesos de usuarios mediante engaño.

Artículo 563. Falsificación de Reservas o Respaldo

Queda prohibido falsear, manipular, ocultar o exagerar reservas, colateral, proof of reserves, auditorías, activos subyacentes, garantías, seguros, respaldo estatal o solvencia de un emisor, plataforma, custodio, stablecoin o activo tokenizado.

Artículo 564. Simulación de Descentralización

Queda prohibido presentar como descentralizado un protocolo, token, plataforma, DAO, exchange, stablecoin o sistema cuando exista control centralizado relevante no divulgado sobre fondos, parámetros, admin keys, liquidez, oráculos, gobernanza, front-end o tesorería.

Artículo 565. Captación Pública Digital no Autorizada

Queda prohibida la captación pública de recursos mediante activos digitales, promesas de rendimiento, pools, vaults, tokens, DAOs, bots, arbitraje, inversión colectiva o plataformas digitales sin autorización cuando, por su naturaleza, constituya actividad regulada.

SECCIÓN VIII — CLÁUSULAS FINALES DE PROTECCIÓN E INTEGRIDAD

Artículo 566. Cláusula de Integridad del Ecosistema

La IID deberá interpretar sus competencias de protección al usuario e integridad de mercado de forma que preserve confianza, transparencia, innovación, autocustodia, competencia, privacidad y acceso legítimo a redes descentralizadas.

Artículo 567. Cláusula Anti Fraude Web3

Será contrario a esta ley todo diseño, comunicación, estructura, contrato, token, protocolo, plataforma o campaña que utilice la complejidad tecnológica para ocultar fraude, riesgos, control efectivo, conflictos de interés, falta de respaldo o apropiación indebida de fondos.

Artículo 568. Cláusula Pro Usuario Soberano

La protección del usuario digital deberá reconocerlo como sujeto capaz de informarse, decidir, asumir riesgos, autocustodiar activos, participar en mercados y exigir transparencia, sin perjuicio de las normas imperativas de protección al consumidor y de integridad de mercado.

La IID ejercerá competencias especiales sobre disclosure Web3, custodia digital, reservas, publicidad de productos dentro de su perímetro, integridad y manipulación de mercados digitales regulados y deberes específicos de los sujetos supervisados.

Las competencias generales en materia de competencia económica, protección general del consumidor y prácticas comerciales permanecerán en las autoridades establecidas por la legislación general, bajo coordinación interinstitucional y sin duplicidad sancionatoria.

CAPÍTULO XIX — RÉGIMEN SANCIONATORIO ADMINISTRATIVO, MEDIDAS CAUTELARES, GARANTÍAS PROCESALES Y DEBIDO PROCESO DIGITAL

SECCIÓN I — PRINCIPIOS FUNDAMENTALES DEL RÉGIMEN SANCIONATORIO DIGITAL

Artículo 569. Principio de Legalidad Digital

Ninguna persona física, jurídica, DAO, protocolo, desarrollador, operador de infraestructura, VASP, mercado, banco digital, emisor, custodio, usuario o participante del ecosistema Web3 podrá ser sancionado administrativamente

sino por una conducta previamente tipificada por ley, sin perjuicio del desarrollo técnico reglamentario expresamente habilitado.

Queda prohibida la creación de infracciones o sanciones mediante guía, circular, criterio interpretativo, práctica administrativa, analogía o interpretación extensiva desfavorable.

Artículo 570. Principio de Tipicidad Estricta

Las infracciones deberán describirse de forma clara, precisa y técnicamente comprensible, indicando la conducta sancionable, el sujeto responsable, el deber incumplido, el grado de culpa o dolo requerido y la sanción aplicable.

La ambigüedad normativa deberá resolverse a favor de la persona investigada cuando exista duda razonable sobre la ilicitud de la conducta.

Artículo 571. Proporcionalidad Tecnológica

Toda sanción o medida restrictiva deberá ser proporcional al riesgo, daño, beneficio obtenido, grado de control efectivo, intencionalidad, reincidencia, cooperación, impacto sobre usuarios, naturaleza técnica de la conducta y capacidad económica del responsable.

No podrá sancionarse de la misma forma:

a) Un fraude doloso.
b) Un error técnico no doloso.
c) Una vulnerabilidad reportada de buena fe.
d) Un experimento fallido.
e) Una falla de smart contract sin ocultamiento.
f) Una pérdida causada por volatilidad de mercado.
g) Una conducta de autocustodia legítima.
h) Una actividad profesional regulada sin licencia.

Artículo 572. Presunción de Licitud Tecnológica

Se presume lícito el uso, desarrollo, publicación, ejecución, auditoría, investigación o interacción con tecnologías blockchain, activos digitales, wallets no custodiales, nodos, validadores, smart contracts, DeFi, software libre, criptografía, ZKP, DAOs e infraestructura descentralizada, salvo prueba de conducta ilícita específica.

SECCIÓN II — INFRACCIONES ADMINISTRATIVAS

Artículo 573. Infracciones Leves

Constituyen infracciones leves, cuando no generen daño grave ni riesgo sistémico:

a) Retrasos menores en reportes regulatorios.
b) Omisiones formales subsanables.
c) Errores no dolosos en documentación.
d) Incumplimientos menores de disclosure.
e) Fallas administrativas sin afectación material a usuarios.
f) Publicación incompleta de información no esencial.
g) Incumplimientos técnicos corregidos oportunamente.
h) Falta de actualización de datos registrales sin mala fe.

Las infracciones leves podrán corregirse mediante apercibimiento, plan de remediación o multa proporcional.

Artículo 574. Infracciones Graves

Constituyen infracciones graves:

a) Operar actividad regulada sin autorización cuando esta sea exigible.
b) Incumplir deberes materiales de disclosure.
c) Publicidad engañosa relevante.
d) Incumplimientos AML/CFT significativos por sujetos obligados.
e) No segregar activos de clientes.
f) Ocultar conflictos de interés materiales.
g) No reportar incidentes relevantes.
h) Listar activos sin evaluación mínima exigida.
i) Fallas graves de ciberseguridad por negligencia.
j) Incumplir órdenes legítimas de la IID.
k) Administrar tesorerías DAO sin reglas mínimas cuando sean exigibles.
l) Incumplir proof of reserves cuando sea obligatorio.

Artículo 575. Infracciones Muy Graves

Constituyen infracciones muy graves:

a) Apropiación indebida de activos de usuarios.
b) Fraude digital organizado.
c) Rug pull doloso.
d) Falsificación de reservas.
e) Manipulación deliberada de mercado.
f) Captación pública no autorizada con engaño.
g) Lavado de dinero o financiamiento ilícito mediante sujetos regulados.
h) Ocultamiento deliberado de insolvencia.
i) Uso indebido de fondos custodiados.
j) Hackeo interno o facilitación dolosa de exploits.
k) Manipulación de oráculos o smart contracts con ánimo de lucro indebido.
l) Simulación dolosa de descentralización.
m) Obstrucción grave a una investigación legítima.
n) Reincidencia en infracciones graves con daño a usuarios.

Artículo 576. Fraude Digital Agravado

Se considerará fraude digital agravado cuando la conducta:

a) Afecte a usuarios minoristas de forma masiva.
b) Utilice identidad falsa o suplantación.
c) Explote vulnerabilidad técnica conocida y ocultada.
d) Use publicidad engañosa coordinada.
e) Involucre fondos de clientes o activos custodiados.
f) Simule respaldo estatal o regulatorio.
g) Use IA, deepfakes o bots para engañar.
h) Oculte concentración de control.
i) Involucre múltiples jurisdicciones para evadir responsabilidad.
j) Afecte infraestructura crítica o mercados regulados.

SECCIÓN III — CONDUCTAS NO SANCIONABLES POR SÍ SOLAS

Artículo 577. No Criminalización de Software Neutral

No será sancionable por sí sola la creación, publicación, auditoría, mantenimiento, distribución, compilación, investigación, enseñanza o ejecución de software blockchain, smart contracts, wallets no custodiales, nodos, validadores, herramientas criptográficas, ZKP, protocolos DeFi o infraestructura open-source.

La responsabilidad surgirá únicamente cuando exista participación dolosa, fraude, control efectivo abusivo, custodia indebida, ocultamiento de riesgos, administración de fondos de terceros o colaboración directa con actividades ilícitas.

Artículo 578. No Sanción por Autocustodia

No será sancionable por sí sola la autocustodia, tenencia, recepción, transferencia, inversión, ahorro, firma de transacciones, uso de hardware wallets, uso de multisig, interacción peer-to-peer o control de llaves privadas sobre activos propios.

Artículo 579. No Responsabilidad por Código Open Source Neutral

Los desarrolladores, auditores, investigadores o contribuidores de código open-source no serán responsables por daños derivados de usos no autorizados, ilícitos o imprevisibles de terceros, salvo que hayan actuado con dolo, fraude, ocultamiento deliberado de vulnerabilidades críticas, control efectivo sobre fondos o participación directa en la conducta ilícita.

Artículo 580. Protección de Investigadores de Seguridad y White Hats

No serán sancionadas las personas que, de buena fe, investiguen, identifiquen, reporten o ayuden a corregir vulnerabilidades de seguridad, siempre que:

a) No exploten abusivamente la vulnerabilidad.
b) No se apropien de fondos.
c) No extorsionen.
d) No destruyan información.
e) No excedan de forma desproporcionada el alcance razonable de la prueba.
f) Realicen divulgación responsable.
g) Cooperen con la corrección cuando sea posible.

SECCIÓN IV — MEDIDAS CAUTELARES DIGITALES

Artículo 581. Principio de Necesidad Cautelar

Toda medida cautelar digital deberá ser necesaria, idónea, proporcional, temporal, motivada y basada en indicios razonables de riesgo concreto.

No podrán adoptarse medidas cautelares por mera sospecha genérica, presión mediática, prejuicio tecnológico o uso legítimo de autocustodia.

Artículo 582. Congelamiento Proporcional de Activos

La IID podrá ordenar cautelarmente a un sujeto regulado bajo su supervisión la inmovilización temporal de activos digitales que dicho sujeto custodie o controle por cuenta propia o de terceros, cuando exista base legal, riesgo concreto e inmediato de pérdida, fraude, apropiación indebida, legitimación de capitales, financiamiento ilícito, manipulación grave, incumplimiento regulatorio sustancial o peligro relevante para usuarios.

La medida deberá ser motivada, individualizada, proporcional y limitada a los activos, cuentas o montos razonablemente vinculados con la conducta investigada. Tendrá una duración inicial máxima de quince días hábiles y podrá renovarse una sola vez mediante resolución motivada cuando persistan las circunstancias que la justificaron, sin perjuicio de las medidas que correspondan a la autoridad judicial o a otras autoridades competentes.

La IID no podrá, por esta sola disposición, intervenir llaves privadas, confiscar activos autocustodiados, bloquear infraestructura neutral ni disponer patrimonios que no se encuentren bajo control de un sujeto regulado. Toda afectación que exceda el ámbito cautelar administrativo requerirá la intervención de la autoridad competente conforme al ordenamiento.

Artículo 583. Prohibición de Bloqueos Masivos de Wallets

Queda prohibido ordenar bloqueos masivos, indiscriminados o preventivos de wallets, protocolos, usuarios o activos digitales sin individualización mínima, justificación técnica y base legal suficiente.

Las medidas deberán evitar afectar usuarios inocentes, pools no relacionados, infraestructura neutral o activos ajenos a la investigación.

Artículo 584. Protección de Usuarios Inocentes

Toda medida cautelar deberá prever mecanismos para proteger a usuarios no involucrados, terceros de buena fe, participantes de pools, holders, proveedores neutrales, usuarios de protocolos y contrapartes legítimas.

Cuando sea posible, la autoridad deberá permitir separación de fondos, reclamación, liberación parcial, prueba de origen o mecanismos de revisión.

Artículo 585. Temporalidad y Revisión de Medidas

Toda medida cautelar tendrá plazo determinado y estará sujeta a revisión periódica. La autoridad deberá levantarla, limitarla o modificarla cuando desaparezca el riesgo, se acredite error, se afecte desproporcionadamente a terceros o se prolongue sin justificación.

SECCIÓN V — DEBIDO PROCESO DIGITAL

Artículo 586. Derecho de Defensa Técnica

Toda persona investigada tendrá derecho a defensa técnica jurídica y, cuando sea necesario, defensa técnica especializada en blockchain, smart contracts, ciberseguridad, criptografía, activos digitales, DeFi, DAOs o infraestructura digital.

Artículo 587. Derecho a Explicación Técnica

La persona investigada tendrá derecho a conocer, en términos razonablemente comprensibles, la base técnica de la imputación, incluyendo:

a) Transacciones relevantes.
b) Direcciones vinculadas.
c) Smart contracts involucrados.
d) Herramientas de análisis utilizadas.
e) Criterios de atribución.
f) Evidencia on-chain.
g) Supuestos de control efectivo.
h) Riesgos identificados.
i) Fuentes de datos utilizadas.

Artículo 588. Derecho a Auditoría y Contraprueba

La persona investigada tendrá derecho a aportar auditorías, análisis on-chain, peritajes, pruebas criptográficas, pruebas de control de wallet, pruebas de origen de fondos, ZKP, documentos, testimonios técnicos y cualquier medio lícito de defensa.

La autoridad deberá valorar la prueba técnica conforme a reglas de sana crítica, especialidad y proporcionalidad.

Artículo 589. Derecho a Revisión Judicial

Toda sanción, medida cautelar, congelamiento, suspensión, revocación de licencia, exclusión, bloqueo, orden correctiva o acto de gravamen emitido por la IID estará sujeto a revisión administrativa y judicial efectiva.

Artículo 590. Transparencia de Enforcement

La IID deberá publicar criterios generales de enforcement, estadísticas de sanciones, tipos de infracciones, montos, tiempos de resolución, medidas adoptadas y resultados agregados, protegiendo datos personales, secretos comerciales e investigaciones en curso.

SECCIÓN VI — SANCIONES Y CRITERIOS DE GRADUACIÓN

Artículo 591. Tipos de Sanciones

La IID podrá imponer, según corresponda:

a) Apercibimiento.
b) Orden de corrección.
c) Plan de remediación.
d) Multa proporcional.
e) Suspensión temporal de actividad regulada.
f) Revocación de licencia.
g) Inhabilitación temporal.
h) Publicación de sanción.
i) Orden de restitución.
j) Compensación a usuarios afectados.
k) Prohibición de operar en mercados regulados.
l) Remisión al Ministerio Público cuando exista delito.

Artículo 592. Criterios de Graduación

Para graduar sanciones se considerará:

a) Gravedad del daño.
b) Número de afectados.
c) Beneficio obtenido.
d) Dolo o culpa.
e) Reincidencia.
f) Cooperación.
g) Remediación voluntaria.
h) Transparencia.
i) Capacidad económica.
j) Riesgo sistémico.
k) Nivel de control efectivo.
l) Impacto sobre innovación.

m) Existencia de disclosure previo.
n) Daño reputacional al ecosistema.
o) Afectación de derechos fundamentales.

Artículo 593. Reparación a Usuarios

Cuando una infracción cause un perjuicio económico directamente verificable a usuarios, la IID podrá ordenar medidas administrativas de restitución, devolución de activos, corrección de balances, reversión de cargos indebidos o restablecimiento de la situación jurídica alterada, cuando dichas medidas se encuentren dentro del ámbito de control del sujeto regulado.

La determinación de indemnizaciones por daños y perjuicios de naturaleza civil corresponderá al acuerdo de las partes, arbitraje o jurisdicción competente. Las medidas administrativas previstas en este artículo no impedirán el ejercicio de acciones civiles o penales.

Artículo 594. Inhabilitación

Podrá imponerse inhabilitación temporal para operar, dirigir, administrar, promover o participar en entidades reguladas cuando exista fraude grave, apropiación indebida, reincidencia, manipulación deliberada, ocultamiento de insolvencia o daño masivo a usuarios.

SECCIÓN VII — DEBANKING, EXCLUSIÓN FINANCIERA Y CENSURA ECONÓMICA

Artículo 595. Protección contra Debanking Arbitrario

Queda prohibido cerrar cuentas, negar servicios, bloquear pagos, cancelar relaciones comerciales o restringir acceso financiero por la sola participación lícita en actividades Web3, blockchain, Bitcoin, autocustodia, minería, validación, DAOs, DeFi, tokenización o activos digitales.

Las entidades financieras deberán basar sus decisiones en análisis individual de riesgo, conducta verificable, cumplimiento normativo y proporcionalidad.

Artículo 596. Derecho de Acceso No Discriminatorio

Las personas y empresas Web3 tendrán derecho a solicitar servicios financieros, bancarios, tecnológicos o de pagos bajo criterios objetivos y no discriminatorios.

La negativa deberá estar basada en razones específicas y no en políticas generales de exclusión del sector.

Artículo 597. Motivación Obligatoria y Revisión

Toda negativa, cierre, bloqueo o restricción significativa deberá ser comunicada con motivación suficiente, salvo impedimento legal justificado, y deberá existir mecanismo de revisión, corrección de falsos positivos y presentación de documentación.

SECCIÓN VIII — COOPERACIÓN INTERNACIONAL GARANTISTA

Artículo 598. Cooperación AML/CFT con Garantías

La cooperación internacional en materia AML/CFT, sanciones, fraude, cibercrimen o abuso de mercado deberá respetar legalidad, debido proceso, proporcionalidad, protección de datos, derechos fundamentales, revisión judicial y prohibición de vigilancia masiva.

Artículo 599. Reconocimiento Limitado de Medidas Extranjeras

Las medidas extranjeras que pretendan producir efectos en Costa Rica sobre activos digitales, wallets, usuarios, protocolos, entidades o mercados deberán ser evaluadas conforme al orden público constitucional costarricense, debido proceso, derechos fundamentales, proporcionalidad y competencia de la autoridad emisora.

No se reconocerán medidas incompatibles con autocustodia legítima, privacidad financiera, libertad digital o prohibición de vigilancia masiva, salvo obligación internacional aplicable y debidamente controlada.

SECCIÓN IX — CLÁUSULAS FINALES DEL ESTADO DE DERECHO DIGITAL

Artículo 600. Cláusula Anti Abuso Regulatorio

Será contrario a esta ley todo uso de potestades regulatorias destinado a perseguir innovación, bloquear competencia, favorecer incumbentes, eliminar autocustodia, censurar financieramente, criminalizar software neutral, imponer vigilancia masiva o sancionar sin base legal clara.

Artículo 601. Cláusula Anti Vigilancia Masiva

Ninguna potestad sancionatoria, cautelar, investigativa o de supervisión podrá interpretarse como autorización para monitoreo indiscriminado de wallets, identificación universal, vigilancia financiera poblacional o perfilamiento masivo de usuarios.

Artículo 602. Cláusula Pro Innovación y Buena Fe

Toda duda razonable en materia sancionatoria deberá interpretarse considerando buena fe, innovación responsable, transparencia del actor, ausencia de daño, ausencia de dolo, cooperación, remediación voluntaria y naturaleza emergente de la tecnología.

Esta cláusula no amparará fraude, ocultamiento, manipulación, abuso de usuarios o simulación de descentralización.

SECCIÓN ESPECIAL — RÉGIMEN PENAL Y SANCIONATORIO REFORZADO PARA LA SOBERANÍA DIGITAL

La presente sección complementa el régimen sancionatorio general del capítulo y establece tipos especiales, criterios de responsabilidad y sanciones agravadas para conductas que comprometan soberanía digital, infraestructura crítica, democracia digital, neuroderechos, inteligencia artificial, computación cuántica, blockchain estatal, identidad digital soberana, ciberseguridad nacional y derechos fundamentales digitales.

CAPÍTULO XX — DERECHO PENAL ESPECIAL, COOPERACIÓN PENAL TÉCNICA Y PROTECCIÓN DE LA SOBERANÍA DIGITAL

SECCIÓN I — PRINCIPIOS DEL DERECHO PENAL DIGITAL ESPECIAL

Artículo 603. Principio de legalidad tecnológica reforzada

Ninguna persona será sancionada penal o administrativamente por el solo hecho de desarrollar, publicar, auditar, investigar, operar o utilizar tecnologías emergentes, blockchain, inteligencia artificial, criptografía, wallets no custodiales, nodos, validadores, smart contracts, software libre, herramientas de privacidad o infraestructura descentralizada lícita.

La responsabilidad penal exigirá conducta típica, antijurídica y culpable en los términos del Código Penal y de los tipos especiales establecidos en este capítulo. La responsabilidad culposa o por negligencia únicamente procederá cuando el tipo penal correspondiente la contemple expresamente.

El incumplimiento de obligaciones regulatorias será objeto del régimen administrativo salvo que la conducta reúna, además, todos los elementos de un tipo penal expresamente previsto por ley.

Artículo 604. Régimen diferenciado de responsabilidad digital

Las conductas reguladas en esta sección podrán generar responsabilidad administrativa, civil, penal, disciplinaria, patrimonial, societaria o regulatoria, según la naturaleza del hecho, el sujeto responsable, el daño causado, el nivel de riesgo sistémico y el grado de afectación a derechos fundamentales.

La imposición de sanciones deberá considerar si la conducta afectó usuarios individuales, consumidores, mercados, infraestructura crítica, servicios públicos esenciales, sistemas electorales, identidad digital soberana, neurodatos, registros públicos, llaves criptográficas estatales, activos públicos tokenizados o estabilidad financiera digital.

Artículo 605. Clasificación de riesgo sistémico digital

Para graduar sanciones, la autoridad competente deberá clasificar el impacto de la conducta en niveles bajo, medio, alto, crítico o sistémico.

Se considerará riesgo crítico o sistémico cuando la conducta comprometa, entre otros: identidad digital nacional, Registro Público blockchain, sistemas electorales, infraestructura cloud estatal, redes de pagos, stablecoins sistémicas, custodios relevantes, datasets soberanos, infraestructura energética digital, neurodatos masivos, llaves criptográficas estatales, servicios públicos esenciales o mercados digitales de relevancia nacional.

Artículo 606. Agravantes especiales en materia tecnológica

Serán agravantes especiales: actuar como autoridad pública o proveedor crítico; abusar de acceso privilegiado; afectar menores de edad; comprometer datos sensibles, biométricos o neurodatos; actuar con ánimo de lucro ilícito; utilizar IA, automatización o infraestructura transfronteriza para aumentar el daño; ocultar vulnerabilidades críticas; destruir evidencia criptográfica; obstruir auditorías; comprometer infraestructura electoral o financiera; o ejecutar la conducta en contexto de emergencia nacional, proceso electoral o incidente cibernético.

Artículo 607. Atenuantes, cooperación y corrección temprana

Podrán considerarse atenuantes la cooperación efectiva, revelación temprana, reparación integral, mitigación inmediata, notificación responsable de vulnerabilidades, ausencia de daño efectivo, implementación de controles posteriores, auditoría independiente voluntaria y colaboración con autoridades competentes.

No procederá atenuante cuando la cooperación sea aparente, tardía, incompleta o utilizada para encubrir destrucción de evidencia, continuidad del daño o transferencia de activos ilícitos.

Artículo 608. Delito de captura tecnológica del Estado

Será sancionada la persona que, mediante fraude, corrupción, colusión, conflicto de interés oculto, dependencia contractual abusiva, manipulación técnica, diseño cerrado deliberado o abuso de posición dominante, capture o intente capturar infraestructura digital crítica del Estado.

La pena será agravada cuando la conducta afecte identidad digital soberana, Registro Público, sistemas electorales, infraestructura de pagos, salud, justicia, seguridad pública, contratación pública, cloud estatal, llaves criptográficas o sistemas de transparencia blockchain.

Artículo 609. Delito de sabotaje de infraestructura digital crítica

Será sancionada la persona que destruya, inutilice, degrade, altere, interrumpa, comprometa o sabotee infraestructura digital crítica nacional, incluyendo sistemas blockchain estatales, registros públicos digitales, infraestructura electoral, cloud soberano, nodos públicos estratégicos, sistemas de pagos, infraestructura energética digital o servicios esenciales.

Cuando el sabotaje cause afectación masiva, riesgo para la seguridad nacional, interrupción de servicios públicos esenciales o pérdida de integridad institucional, la conducta será considerada de máxima gravedad.

Artículo 610. Delito de manipulación de infraestructura electoral digital

Será sancionada la persona que altere, manipule, interfiera, destruya, falsee, suprima, infiltre o comprometa sistemas electorales digitales, registros electorales, transmisión de resultados, auditorías criptográficas, credenciales electorales, hashes, actas digitales, conteo automatizado o infraestructura de verificación democrática.

La utilización de IA, deepfakes, bots, microsegmentación opaca, falsificación de evidencia digital o proveedores tecnológicos no auditables para alterar la voluntad electoral constituirá agravante especial.

Artículo 611. Delito de extracción ilícita de datasets soberanos

Será sancionada la extracción, copia, transferencia, venta, entrenamiento algorítmico, explotación o acceso no autorizado a datasets soberanos del Estado o de interés estratégico nacional.

Se considerarán especialmente protegidos los datasets electorales, biométricos, sanitarios, financieros públicos, tributarios, judiciales, registrales, educativos, de seguridad nacional, infraestructura crítica, identidad digital soberana y datos utilizados para entrenamiento de IA sobre población costarricense.

Artículo 612. Delito de interferencia ilícita en infraestructura cloud crítica

Será sancionada la persona que, sin autorización o excediendo la otorgada, acceda, manipule, interrumpa, degrade, extraiga, transfiera, bloquee, cifre, destruya o comprometa infraestructura cloud utilizada por el Estado, servicios públicos esenciales, operadores críticos, sistemas financieros digitales, identidad soberana o registros estratégicos.

Será agravante actuar desde infraestructura extranjera, ocultar subprocesadores críticos, impedir reversibilidad contractual, retener datos públicos o comprometer llaves criptográficas estatales.

Artículo 613. Delito de manipulación de identidad digital soberana

Será sancionada la creación, alteración, revocación, bloqueo, suplantación, transferencia, venta, correlación abusiva o explotación ilícita de identidad digital soberana, credenciales verificables, DID, wallets de identidad, atributos estatales o mecanismos de autenticación de una persona.

La pena será agravada cuando la conducta cause exclusión de servicios públicos, pérdida patrimonial, afectación electoral, discriminación, vigilancia, acceso indebido a datos sensibles o bloqueo de participación económica digital.

Artículo 614. Delito de manipulación algorítmica masiva

Será sancionada la persona que diseñe, despliegue, financie, comercialice o utilice sistemas de inteligencia artificial o automatización destinados a manipular masivamente conducta, opinión, preferencias, decisiones económicas, participación política, consumo, acceso financiero o derechos de una población, mediante engaño, ocultamiento, explotación de vulnerabilidades o abuso de datos.

La conducta será agravada cuando afecte menores de edad, procesos electorales, salud mental, neurodatos, servicios públicos esenciales o estabilidad financiera.

Artículo 615. Delito de scoring social ilegal

Será sancionada la creación, operación, comercialización o integración de sistemas de scoring social destinados a clasificar personas para otorgar o restringir derechos, servicios, crédito, empleo, educación, movilidad, participación política, identidad, acceso digital o beneficios públicos con base en comportamiento, ideología, reputación, asociaciones, actividad financiera, datos biométricos, neurodatos o historial digital.

Artículo 616. Delito de deepfakes electorales y contenido sintético fraudulento

Será sancionada la producción, distribución o financiamiento malicioso de contenido sintético, deepfakes, clonación de voz, imagen o identidad digital, cuando se utilice para manipular procesos electorales, suplantar autoridades, falsificar comunicaciones oficiales, inducir fraude, afectar mercados, alterar confianza pública o vulnerar derechos fundamentales.

La sanción será mayor cuando el contenido sea difundido durante procesos electorales, emergencias nacionales o crisis financieras.

Artículo 617. Delito de ingeniería cognitiva mediante IA

Será sancionada la utilización de IA para explotación deliberada de vulnerabilidades cognitivas, emocionales, psicológicas o neurobiológicas de personas o grupos, con el fin de inducir dependencia, alterar decisiones relevantes, obtener consentimiento manipulado, condicionar preferencias políticas o económicas o vulnerar autonomía mental.

Cuando la conducta afecte menores de edad, personas en situación de vulnerabilidad o neurodatos, tendrá carácter agravado.

Artículo 618. Delito de fraude masivo mediante inteligencia artificial

Será sancionada la utilización de IA, agentes autónomos, modelos generativos, automatización, bots o sistemas sintéticos para cometer fraude masivo, suplantación, phishing, manipulación de mercados, falsificación documental, captación engañosa, simulación de respaldo, falsificación de auditorías, falsas pruebas de reservas o estafas sobre activos digitales.

Artículo 619. Delito de automatización financiera abusiva

Será sancionada la implementación deliberada de sistemas automatizados que bloqueen, congelen, excluyan, censuren, liquiden, ejecuten garantías, restrinjan wallets, nieguen acceso financiero o alteren posiciones patrimoniales sin base legal, sin contrato válido, sin transparencia, sin revisión humana cuando corresponda o mediante abuso de posición dominante.

Artículo 620. Delito de IA para vigilancia ilícita

Será sancionada la utilización de IA para vigilancia masiva, reconocimiento biométrico indiscriminado, perfilamiento político, monitoreo financiero generalizado, correlación masiva de identidad, seguimiento conductual o extracción de patrones personales sin base legal suficiente y garantías constitucionales.

Artículo 621. Delito de extracción ilegal de neurodatos

Será sancionada la recolección, acceso, copia, inferencia, transferencia, venta, entrenamiento algorítmico, explotación o tratamiento de neurodatos sin consentimiento válido, base legal suficiente o finalidad legítima.

La sanción será agravada cuando los neurodatos provengan de menores, pacientes, trabajadores, estudiantes, personas privadas de libertad, consumidores bajo presión o usuarios sometidos a asimetría tecnológica significativa.

Artículo 622. Delito de interferencia neurotecnológica o brain hacking

Será sancionada la interferencia, intrusión, manipulación, alteración, sabotaje o acceso no autorizado a interfaces cerebro-computadora, dispositivos neuronales, sistemas de estimulación cerebral, implantes, sensores neurotecnológicos o plataformas que procesen actividad cerebral.

La conducta será agravada si produce daño físico, psicológico, cognitivo, pérdida de autonomía, alteración de voluntad, afectación de memoria, dependencia tecnológica o riesgo para la vida o salud.

Artículo 623. Delito de neuroperfilamiento y neuromarketing ilícito

Será sancionado el uso de neurodatos, inferencias mentales, patrones cognitivos, emociones detectadas o respuestas neurofisiológicas para segmentación, publicidad, propaganda, manipulación comercial, política, educativa o laboral sin consentimiento reforzado o con finalidad abusiva.

Se prohíbe especialmente el neuromarketing dirigido a menores de edad o poblaciones vulnerables cuando explote su desarrollo cognitivo o emocional.

Artículo 624. Delito de modificación conductual no consentida

Será sancionada toda intervención tecnológica, neurotecnológica, algorítmica o combinada destinada a modificar conducta, preferencias, atención, memoria, emociones, impulsos o decisiones relevantes sin consentimiento válido, información suficiente y supervisión adecuada cuando corresponda.

Artículo 625. Delito de compromiso criptográfico mediante capacidades cuánticas

Será sancionada la utilización de computación cuántica, técnicas post-cuánticas ofensivas o capacidades equivalentes para comprometer cifrado, firmas digitales, llaves criptográficas, wallets, infraestructura estatal, identidad digital, registros blockchain, comunicaciones protegidas o activos digitales sin autorización legal.

Artículo 626. Delito de ataque post-cuántico contra infraestructura soberana

Será sancionada toda conducta que utilice capacidades computacionales avanzadas para degradar, falsificar, romper, sustituir o neutralizar infraestructura criptográfica de sistemas estatales, electorales, registrales, financieros, sanitarios, judiciales o de infraestructura crítica.

La sanción será agravada cuando exista afectación a seguridad nacional, sistemas electorales, llaves estatales, registros públicos o estabilidad financiera digital.

Artículo 627. Responsabilidad por omisión grave de protección post-cuántica

Los operadores de infraestructura crítica digital, custodios sistémicos, proveedores cloud críticos, emisores relevantes, registros públicos digitales y autoridades tecnológicas podrán ser sancionados cuando omitan de forma grave e injustificada planes razonables de transición, evaluación o mitigación frente a riesgos criptográficos post-cuánticos previamente identificados por autoridad competente.

Artículo 628. Delito de manipulación de registro blockchain estatal

Será sancionada la persona que altere, suprima, falsifique, reordene, oculte, duplique, bloquee o manipule registros blockchain estatales, hashes, sellos de tiempo, evidencias criptográficas, actas digitales, certificaciones verificables o trazas institucionales.

La sanción será agravada cuando la conducta afecte Registro Público, catastro, contratación pública, presupuesto, deuda, concesiones, justicia, elecciones, salud o activos públicos tokenizados.

Artículo 629. Delito de corrupción de smart contracts estatales

Será sancionada la persona que introduzca, explote, oculte o mantenga deliberadamente vulnerabilidades, puertas traseras, reglas abusivas, oráculos manipulables, funciones ocultas o privilegios indebidos en smart contracts estatales o de infraestructura pública.

Cuando el hecho permita desvío de fondos, alteración de adjudicaciones, manipulación de registros, ejecución indebida de pagos o afectación de derechos, constituirá agravante especial.

Artículo 630. Delito de falsificación de credenciales verificables y fe pública criptográfica

Será sancionada la emisión, alteración, venta, uso o presentación fraudulenta de credenciales verificables, certificados digitales, firmas criptográficas, DID, tokens de identidad, constancias públicas, pruebas de cumplimiento o documentos electrónicos interoperables.

La sanción será agravada cuando se utilicen para obtener licencias, servicios financieros, identidad electoral, beneficios públicos, acceso a infraestructura crítica o autorización regulatoria.

Artículo 631. Delito de manipulación de oráculos públicos o críticos

Será sancionada la manipulación dolosa de oráculos, feeds de datos, índices, precios, parámetros externos, sensores, datos de mercado, datos ambientales, datos electorales, datos registrales o fuentes de información utilizadas por smart contracts públicos, mercados digitales o sistemas automatizados de relevancia crítica.

Artículo 632. Sanciones administrativas por riesgo sistémico digital

Las infracciones administrativas vinculadas a infraestructura crítica, custodios sistémicos, stablecoins relevantes, mercados digitales, proveedores cloud críticos, operadores de identidad soberana, sistemas de IA de alto impacto o servicios esenciales podrán sancionarse con multas agravadas, suspensión de operaciones, intervención técnica temporal, revocatoria de autorización, inhabilitación, órdenes de mitigación, auditoría forense y publicación de la sanción.

La multa podrá graduarse según ingresos brutos, volumen de activos, número de usuarios afectados, beneficio obtenido, riesgo sistémico, reincidencia y cooperación.

Artículo 633. Responsabilidad personal de directores y administradores

Los directores, administradores, representantes, beneficiarios controlantes y altos ejecutivos responderán personalmente cuando autoricen, toleren, encubran o no impidan, teniendo deber jurídico de hacerlo, conductas graves que comprometan usuarios, activos, datos, infraestructura crítica, neurodatos, mercados, sistemas electorales, identidad digital o estabilidad financiera.

La responsabilidad personal requerirá dolo, culpa grave, incumplimiento deliberado de deberes fiduciarios, omisión consciente de controles o beneficio directo o indirecto.

Artículo 634. Responsabilidad de responsables tecnológicos y compliance officers

Los responsables tecnológicos, oficiales de cumplimiento, responsables de seguridad, auditores internos, custodios de llaves o encargados de riesgo podrán responder cuando oculten vulnerabilidades críticas, falseen reportes, simulen controles, omitan alertas graves, destruyan evidencia, faciliten incumplimientos o permitan continuidad de riesgos sistémicos conocidos.

No responderán por simples fallas técnicas inevitables ni por decisiones superiores que hayan advertido de forma documentada.

Artículo 635. Deber reforzado de ciberseguridad

Los sujetos regulados de alto impacto deberán implementar controles razonables de ciberseguridad, gestión de incidentes, protección de llaves, segregación de funciones, monitoreo proporcional, pruebas de resiliencia, respaldo, continuidad operativa, auditoría, capacitación y respuesta ante vulnerabilidades.

El incumplimiento grave de estos deberes será sancionado cuando cause o aumente exposición de usuarios, pérdida de activos, filtración de datos sensibles, compromiso de infraestructura crítica o afectación sistémica.

Artículo 636. Responsabilidad por exposición masiva de datos o llaves

Será sancionada la exposición, pérdida, filtración, publicación, venta, transferencia o compromiso de datos personales sensibles, neurodatos, credenciales verificables, datos biométricos, llaves privadas, seed phrases, claves estatales o información crítica, cuando derive de dolo, culpa grave, ausencia de controles razonables o incumplimiento de deberes regulatorios.

Artículo 637. Responsabilidad por auditoría defectuosa o falsa de smart contracts

Los auditores de smart contracts, pruebas de reservas, oráculos, sistemas blockchain, IA, cloud o infraestructura crítica responderán cuando emitan informes falsos, oculten vulnerabilidades materiales, simulen pruebas, certifiquen sin revisión razonable o actúen con conflicto de interés no revelado.

La responsabilidad no se extenderá a errores técnicos razonables cuando se haya actuado con diligencia profesional, límites de alcance claros y revelación adecuada.

Artículo 638. Deber de revelación responsable de vulnerabilidades críticas

Los operadores críticos, VASP, custodios, emisores relevantes, mercados digitales, proveedores cloud, sistemas públicos y desarrolladores responsables deberán contar con mecanismos de recepción, evaluación y mitigación de vulnerabilidades críticas.

La revelación responsable de buena fe de vulnerabilidades no será sancionada cuando se realice sin explotación indebida, sin extorsión, sin apropiación de datos o activos y con finalidad de mitigación.

Artículo 639. Delito de Vigilancia Masiva Digital Ilícita

La implementación, contratación, financiamiento u operación de sistemas de vigilancia masiva, perfilamiento conductual generalizado, scoring social, trazabilidad financiera indiscriminada, identidad centralizada coercitiva o reconocimiento biométrico masivo sin base legal suficiente constituirá infracción gravísima y, cuando corresponda, delito contra derechos fundamentales digitales.

Las autoridades responsables podrán quedar sujetas a responsabilidad administrativa, civil, penal, disciplinaria, patrimonial e inhabilitación para ejercer cargos públicos o contratar con el Estado.

Artículo 640. Sanción por trazabilidad financiera abusiva

Será sancionada la creación u operación de sistemas que permitan monitoreo financiero masivo, correlación injustificada de wallets, perfilamiento económico total, censura transaccional automatizada o bloqueo patrimonial sin base legal, debido proceso y proporcionalidad.

El cumplimiento AML/CFT legítimo no podrá utilizarse como cobertura para vigilancia financiera generalizada.

Artículo 641. Sanción por identidad digital centralizada coercitiva

Será sancionada la autoridad, proveedor o entidad que imponga identidad digital única, centralizada u obligatoria como condición general para ejercer derechos, acceder a servicios esenciales, participar en economía digital, votar,

estudiar, trabajar, comunicarse o utilizar medios de pago lícitos, salvo habilitación legal estricta y proporcional para finalidades específicas.

Artículo 642. Medidas cautelares tecnológicas reforzadas

Ante riesgo grave, actual o inminente para soberanía digital, usuarios, infraestructura crítica, datos sensibles, neurodatos, sistemas electorales, mercados, llaves criptográficas o derechos fundamentales, la autoridad competente podrá ordenar medidas cautelares proporcionales, motivadas y revisables.

Podrán incluir suspensión temporal de sistemas, preservación de evidencia, auditoría forense, congelamiento regulado de operaciones específicas, obligación de notificación, rotación de llaves, desconexión segura, respaldo, mitigación técnica, prohibición de destrucción de registros o designación de interventor técnico.

Artículo 643. Garantías procesales en enforcement tecnológico

Todo procedimiento sancionatorio tecnológico deberá garantizar legalidad, tipicidad, motivación, proporcionalidad, presunción de inocencia, acceso al expediente, defensa técnica, contradicción de prueba digital, peritaje independiente, revisión humana, impugnación, tutela judicial efectiva y protección contra sanciones automatizadas irrevisables.

Artículo 644. Reparación integral, restitución y remediación tecnológica

Las sanciones podrán incluir reparación integral a víctimas, restitución de activos, compensación económica, restauración de credenciales, corrección de datos, eliminación de perfiles ilícitos, reconstrucción de registros, auditoría correctiva, publicación de rectificación, fortalecimiento de controles y financiamiento de medidas de remediación.

Artículo 645. Protección de denunciantes y auditores de buena fe

Se protegerá a denunciantes, auditores, investigadores, empleados, usuarios, desarrolladores o funcionarios que informen de buena fe sobre vulnerabilidades, fraude, vigilancia masiva, corrupción tecnológica, captura institucional, manipulación algorítmica, riesgos sistémicos o delitos digitales.

Queda prohibida la represalia laboral, contractual, financiera, tecnológica o reputacional contra denunciantes de buena fe.

Artículo 646. Coordinación con Ministerio Público, Poder Judicial y autoridades técnicas

La IID, autoridades de ciberseguridad, protección de datos, autoridad electoral constitucionalmente competente, supervisores financieros, Poder Judicial, Ministerio Público y demás órganos competentes deberán coordinar protocolos de investigación, preservación de evidencia digital, análisis forense, cooperación internacional, peritaje criptográfico, protección de víctimas y recuperación de activos.

Dicha coordinación deberá respetar independencia judicial, protección de datos, secreto profesional, debido proceso y límites constitucionales a la vigilancia.

Artículo 647. Cláusula final del régimen sancionatorio de soberanía digital

Las disposiciones de esta sección deberán interpretarse de forma armónica con los derechos fundamentales digitales, la libertad de innovación, la protección de autocustodia, el software libre, la privacidad criptográfica, el cumplimiento AML/CFT proporcional, la protección de menores, los neuroderechos, la soberanía energética digital, la seguridad nacional y la tutela judicial efectiva.

Ninguna sanción podrá utilizarse para criminalizar tecnologías neutrales, investigación legítima, autocustodia, operación de nodos, desarrollo de software, privacidad lícita o participación peer-to-peer sin conducta ilícita específica.

SECCIÓN II — PENAS, AGRAVANTES Y GARANTÍAS PENALES ESPECIALES

Artículo 648. Penas Aplicables a Delitos de Soberanía Digital y Tecnológica

Las penas aplicables a los delitos tipificados en los artículos 608 a 631 serán las siguientes, sin perjuicio de una pena mayor establecida por otra ley para la misma conducta:

a) Prisión de dos a seis años para los delitos previstos en los artículos 611, 613, 615, 616, 623, 624 y 630, cuando no concurra una agravante especial.

b) Prisión de cuatro a diez años para los delitos previstos en los artículos 608, 609, 610, 612, 614, 617, 618, 619, 620, 621, 622, 625, 628, 629 y 631, así como para cualquiera de los delitos del inciso anterior cuando afecte infraestructura crítica digital, sistemas electorales, identidad digital soberana, Registro Público, infraestructura de pagos, neurodatos, datos de personas menores de edad, salud, justicia, seguridad nacional o estabilidad financiera digital.

c) Prisión de seis a doce años para el delito previsto en el artículo 626 y para las conductas de los incisos anteriores cuando produzcan interrupción grave de servicios esenciales, afectación masiva, daño patrimonial grave, manipulación democrática efectiva, compromiso de llaves criptográficas estatales, extracción sistemática de datos sensibles o riesgo grave y concreto para la soberanía digital nacional.

El artículo 627 solo generará responsabilidad penal cuando el propio tipo establezca expresamente la conducta culposa o gravemente negligente y se acredite un deber jurídico específico de protección, previsibilidad del riesgo y relación causal con el resultado. Las sanciones administrativas previstas en los artículos 632 a 647 se regirán por el capítulo administrativo y no podrán convertirse en pena penal por analogía.

Artículo 649. Penas Especiales por Delitos contra Blockchain Estatal y Fe Pública Criptográfica

La manipulación dolosa de registros blockchain estatales, hashes oficiales, sellos de tiempo, smart contracts públicos, credenciales verificables oficiales, oráculos públicos o infraestructura de fe pública criptográfica será sancionada con pena de prisión de cuatro a ocho años.

La pena será de seis a doce años cuando la conducta afecte propiedad registral, contratación pública, actos notariales, deuda pública tokenizada, certificaciones estatales, identidad digital soberana o registros vinculados a derechos fundamentales.

Además de la pena principal, el tribunal podrá imponer inhabilitación especial de tres a diez años para contratar con el Estado, administrar infraestructura crítica digital, auditar sistemas públicos o ejercer cargos técnicos vinculados a sistemas afectados.

Artículo 650. Penas Especiales por Delitos de IA, Manipulación Algorítmica y Deepfakes Electorales

Los delitos de manipulación algorítmica masiva, scoring social ilícito, deepfakes electorales, ingeniería cognitiva mediante IA, fraude masivo automatizado, vigilancia algorítmica ilícita o automatización financiera abusiva serán sancionados con pena de prisión de tres a ocho años.

Cuando dichas conductas afecten procesos electorales, menores de edad, consumidores vulnerables, servicios públicos esenciales, estabilidad financiera, derechos fundamentales o seguridad nacional, la pena será de cinco a doce años.

La responsabilidad penal no recaerá sobre el desarrollo neutral de sistemas de inteligencia artificial, investigación académica, auditoría de seguridad o pruebas controladas de buena fe, salvo dolo, fraude, abuso deliberado o daño antijurídico grave.

Artículo 651. Penas Especiales por Delitos sobre Neurodatos y Neurotecnología

La extracción ilícita, transferencia no autorizada, comercialización abusiva, entrenamiento algorítmico ilegítimo, interferencia neurotecnológica, brain hacking, neuroperfilamiento ilícito, neuromarketing coercitivo o modificación conductual no consentida será sancionada con pena de prisión de cuatro a diez años.

La pena será de seis a doce años cuando la víctima sea menor de edad, paciente, estudiante, trabajador bajo subordinación, persona adulta mayor, persona con discapacidad, persona privada de libertad o persona sometida a especial vulnerabilidad tecnológica, médica, laboral, educativa o económica.

Artículo 652. Penas Especiales por Delitos Financieros Digitales Sistémicos

Los delitos de rug pull sofisticado, extracción maliciosa de liquidez, manipulación fraudulenta de stablecoins, falsificación de reservas, governance exploit, bridge exploit, manipulación de oráculos críticos, fraude mediante smart contracts, simulación de descentralización con captación pública o abuso de infraestructura OTC institucional serán sancionados con pena de prisión de tres a ocho años.

La pena será de cinco a doce años cuando la conducta afecte a múltiples usuarios, infraestructura financiera digital relevante, estabilidad de mercado, fondos de clientes, reservas de stablecoins, liquidez sistémica, activos públicos tokenizados o cooperación financiera internacional.

Artículo 653. Agravantes Especiales del Derecho Penal Digital

Serán agravantes especiales, sin perjuicio de otras previstas por ley: a) afectar infraestructura crítica digital; b) comprometer datos de menores, neurodatos o datos biométricos; c) utilizar inteligencia artificial para ocultar, escalar o automatizar el delito; d) actuar mediante organización transnacional; e) abusar de cargo público, posición regulada o función de auditoría; f) comprometer llaves criptográficas estatales o de clientes; g) afectar procesos electorales; h) causar daño masivo a usuarios; i) utilizar simulación de descentralización para evadir responsabilidad; j) obstaculizar deliberadamente investigación administrativa o penal.

Artículo 654. Atenuantes, Cooperación Eficaz y Remediación Tecnológica

Podrán considerarse atenuantes la cooperación temprana, devolución integral de activos, preservación de evidencia, corrección técnica inmediata, revelación responsable de vulnerabilidades, colaboración eficaz con autoridades, reparación a usuarios, mitigación de daño sistémico y ausencia de beneficio económico ilegítimo.

La atenuación no procederá cuando exista afectación deliberada a menores, neurodatos, procesos electorales, infraestructura crítica, seguridad nacional o derechos fundamentales esenciales.

SECCIÓN III — IID COMO ÓRGANO TÉCNICO AUXILIAR ESPECIALIZADO

Artículo 655. Naturaleza Auxiliar Técnica de la IID en Materia Penal

La IID podrá actuar como órgano técnico auxiliar especializado del Estado en investigaciones relacionadas con activos digitales, blockchain, tecnologías DLT, smart contracts, stablecoins, infraestructura de liquidación fiat-digital, identidad digital soberana, inteligencia artificial, neurotecnología, ciberseguridad, infraestructura crítica digital y tecnologías emergentes.

Esta función no le confiere potestad de acusar penalmente, dirigir investigaciones penales, juzgar, condenar, imponer penas privativas de libertad ni sustituir al Ministerio Público, al OIJ o al Poder Judicial.

Artículo 656. Unidad de Inteligencia y Análisis Tecnológico de la IID

Créase dentro de la IID la Unidad de Inteligencia y Análisis Tecnológico, como unidad técnica especializada para análisis blockchain, trazabilidad digital, stablecoin flows, smart contracts, DAOs, oráculos, bridges, IA aplicada a mercados digitales, neurotecnología, infraestructura crítica, ciberseguridad, custodia criptográfica y evidencia tecnológica compleja.

La Unidad podrá elaborar informes técnicos, mapas de riesgo, análisis de exposición ilícita, reportes de integridad de mercado, diagnósticos de infraestructura crítica, análisis de smart contracts, evaluaciones de stablecoins, trazabilidad on-chain y criterios técnicos para autoridades competentes, conforme a la ley y con respeto a derechos fundamentales.

Artículo 657. Deber de Remisión al Ministerio Público

Cuando la IID, en ejercicio de sus competencias administrativas, regulatorias, supervisoras o técnicas, detecte hechos que pudieran constituir delito, deberá remitir los antecedentes al Ministerio Público, acompañando, cuando corresponda, informe técnico preliminar, evidencia disponible, trazabilidad relevante, identificación de riesgos y medidas urgentes recomendadas.

La remisión no implicará prejuzgamiento penal ni sustitución de la investigación penal, y deberá respetar presunción de inocencia, confidencialidad, cadena de custodia, protección de datos personales y debido proceso.

Artículo 658. Informes Técnicos Especializados y Valor Auxiliar

Los informes técnicos emitidos por la IID podrán ser utilizados como insumo auxiliar por el Ministerio Público, OIJ, Poder Judicial, UIF y demás autoridades competentes, sin perjuicio de la valoración probatoria conforme a las reglas procesales aplicables.

Dichos informes podrán versar sobre arquitectura de protocolos, trazabilidad blockchain, exposición a wallets de riesgo, funcionamiento de smart contracts, mecanismos de gobernanza, concentración de validadores, proof of reserves, manipulación de oráculos, flujo de stablecoins, operación de DAOs, evidencia criptográfica, infraestructura cloud crítica, IA o neurotecnología.

Artículo 659. Cadena de Custodia Digital y Preservación de Evidencia Tecnológica

La IID, cuando actúe como auxiliar técnico, deberá aplicar protocolos de preservación de evidencia digital, incluyendo cadena de custodia, integridad criptográfica, hashes, sellos de tiempo, documentación de fuentes, conservación de logs, resguardo de metadatos, trazabilidad de accesos, control de versiones y medidas de protección de datos sensibles.

La alteración, pérdida, manipulación o divulgación indebida de evidencia tecnológica por funcionarios, peritos, consultores o terceros autorizados generará responsabilidad administrativa, civil o penal conforme a la ley.

Artículo 660. Mesa Nacional de Coordinación contra Delitos de Infraestructura Digital y Activos Digitales

Créase la Mesa Nacional de Coordinación contra Delitos de Infraestructura Digital y Activos Digitales, como mecanismo de coordinación técnica entre el Ministerio Público, OIJ, IID, UIF, MICITT, BCCR, SUGEF, autoridad electoral constitucionalmente competente, PRODHAB, SUTEL y demás autoridades competentes según la materia.

La Mesa tendrá funciones de coordinación, intercambio técnico, protocolos de actuación, capacitación, alertas tempranas, preservación de evidencia, cooperación internacional, análisis de tipologías, protección de infraestructura crítica y respuesta ante eventos sistémicos, sin sustituir las competencias legales de cada institución.

Artículo 661. Capacitación Especializada del Ministerio Público, OIJ y Poder Judicial

El Estado deberá promover capacitación especializada y continua para fiscales, jueces, defensores públicos, investigadores judiciales, peritos, funcionarios de la IID y autoridades competentes en materia de blockchain, activos digitales, stablecoins, smart contracts, DAOs, IA, neurotecnología, ciberseguridad, evidencia criptográfica, análisis forense digital y tecnologías emergentes.

La IID podrá colaborar técnicamente en dichos programas, en coordinación con el Poder Judicial, Ministerio Público, OIJ, Escuela Judicial, universidades y organismos internacionales.

Artículo 662. Límites Constitucionales a la Cooperación Penal Técnica

Toda cooperación técnica de la IID con autoridades penales deberá respetar legalidad, competencia, proporcionalidad, protección de datos, secreto profesional, reserva de investigación, presunción de inocencia, derecho de defensa, cadena de custodia, control judicial cuando corresponda y prohibición de vigilancia masiva.

La IID no podrá utilizar su función auxiliar para realizar investigaciones penales paralelas, persecución selectiva, perfilamiento masivo, bloqueo extrajudicial de activos, acceso indebido a datos sensibles, debilitamiento criptográfico o sustitución de competencias del Ministerio Público y Poder Judicial.

CAPÍTULO XXI — RESOLUCIÓN DE CONTROVERSIAS, ARBITRAJE DIGITAL, JURISDICCIÓN Y EVIDENCIA CRIPTOGRÁFICA

SECCIÓN I — PRINCIPIOS FUNDAMENTALES

Artículo 663. Reconocimiento de Relaciones Jurídicas Digitales

El Estado reconoce la validez de relaciones jurídicas celebradas, ejecutadas, registradas, verificadas o documentadas mediante blockchain, smart contracts, firmas criptográficas, wallets, credenciales verificables, DAOs, identidad digital soberana y demás tecnologías descentralizadas.

La forma digital, programable, criptográfica o descentralizada de una relación jurídica no afectará por sí sola su validez, exigibilidad o fuerza probatoria, siempre que concurran consentimiento, capacidad, objeto lícito, causa legítima y demás requisitos aplicables conforme a la ley.

Artículo 664. Validez Jurídica de Smart Contracts

Los smart contracts serán reconocidos como mecanismos válidos para expresar, automatizar, ejecutar, verificar o registrar obligaciones, condiciones, pagos, transferencias, garantías, derechos, votaciones, certificaciones, liquidaciones o eventos jurídicos.

Un smart contract podrá tener efectos jurídicos cuando refleje voluntad válida, reglas determinables, objeto lícito y posibilidad de atribuir consentimiento o participación a una persona, entidad, wallet, DAO o mecanismo reconocido.

La ejecución automática de un smart contract no impedirá revisión jurídica posterior cuando exista fraude, error esencial, vulnerabilidad, abuso, incapacidad, nulidad, ilicitud, afectación a terceros o violación de derechos fundamentales.

Artículo 665. Neutralidad Tecnológica Probatoria

Ningún medio de prueba será rechazado únicamente por haberse generado, conservado, firmado, registrado o verificado mediante blockchain, criptografía, smart contracts, wallets, credenciales verificables, ZKP, sistemas descentralizados o infraestructura digital.

Los jueces, árbitros, autoridades administrativas y órganos de control deberán valorar la evidencia digital conforme a autenticidad, integridad, trazabilidad, fiabilidad técnica, cadena de custodia, contexto y reglas de sana crítica.

SECCIÓN II — EVIDENCIA DIGITAL Y CRIPTOGRÁFICA

Artículo 666. Evidencia On-Chain

Se reconoce como evidencia on-chain toda información verificable registrada en blockchain o registros distribuidos, incluyendo transacciones, bloques, hashes, direcciones, firmas, eventos de smart contracts, snapshots, votaciones, ejecuciones, transferencias, logs, propuestas DAO, timestamps y estados de contratos inteligentes.

La evidencia on-chain podrá acreditar hechos técnicos como existencia de una transacción, secuencia temporal, ejecución de un smart contract, interacción con una wallet, participación en gobernanza, transferencia de activos, movimientos de tesorería, anclaje de documentos, integridad de registros o control técnico de una dirección.

El control técnico de una llave, wallet o dirección no constituirá por sí solo prueba irrebatible de identidad, titularidad jurídica o voluntad negocial. Su valor deberá apreciarse junto con las demás circunstancias del caso, incluyendo posibles esquemas multisig, automatización, agencia, custodia, compromiso de llaves o prueba en contrario.

Artículo 667. Firmas Criptográficas

Las firmas criptográficas podrán ser reconocidas como medio válido para acreditar control de una llave privada, consentimiento, autenticación, autorización, recepción, aprobación o participación en un acto digital.

Su valor jurídico dependerá del contexto, del sistema utilizado, del grado de seguridad, de la relación entre llave e identidad, de la intención manifestada y de las circunstancias del caso.

Artículo 668. Wallet Signatures y Consentimiento

La firma de mensajes, transacciones o instrucciones mediante una wallet podrá constituir prueba de consentimiento, autorización o participación cuando:

a) La persona controle legítimamente la wallet.
b) El mensaje o transacción sea comprensible o verificable.
c) Exista contexto suficiente para atribuir intención jurídica.
d) No medie fraude, suplantación, phishing, malware, coacción o error esencial.
e) El sistema permita verificar integridad y autenticidad.

La simple conexión de una wallet a una interfaz no constituirá por sí sola aceptación de obligaciones sustanciales no divulgadas.

Artículo 669. Validez de Registros Blockchain

Los registros blockchain podrán utilizarse como prueba de integridad, existencia, secuencia temporal, ejecución, titularidad técnica o trazabilidad, sin perjuicio de que su alcance jurídico dependa del derecho sustantivo aplicable.

Cuando un registro blockchain represente un activo, derecho o documento off-chain, deberá probarse la relación jurídica entre el registro digital y el activo, derecho o documento subyacente.

Artículo 670. Pruebas de Conocimiento Cero y Divulgación Selectiva

Las pruebas de conocimiento cero, credenciales verificables y mecanismos de divulgación selectiva podrán ser admitidos para acreditar condiciones, atributos, elegibilidad, cumplimiento, no exposición a sanciones, mayoría de edad, solvencia, residencia, titularidad o ausencia de determinados riesgos sin revelar información innecesaria.

La autoridad no podrá rechazar una prueba criptográfica por el solo hecho de preservar privacidad, siempre que sea técnicamente verificable y suficiente para la finalidad probatoria.

SECCIÓN III — SMART CONTRACTS Y EJECUCIÓN PROGRAMABLE

Artículo 671. Ejecución Automatizada

La ejecución automatizada de obligaciones mediante smart contracts será válida cuando derive de una relación jurídica lícita, consentimiento válido y reglas previamente determinadas o determinables.

La ejecución automatizada podrá comprender pagos, transferencias, liquidaciones, liberación de garantías, distribución de ingresos, votaciones, entregas contra pago, condiciones suspensivas, condiciones resolutorias y demás actos permitidos por ley.

Artículo 672. Smart Contracts Híbridos

Se reconocen los smart contracts híbridos, integrados por código ejecutable y documentación legal off-chain, términos de servicio, contratos escritos, documentos de tokenización, estatutos DAO o cláusulas complementarias.

En caso de conflicto entre código y texto legal, deberá atenderse a la voluntad de las partes, reglas de interpretación contractual, protección de consumidores, buena fe, disclosure y finalidad económica del acuerdo.

Artículo 673. Bugs, Vulnerabilidades y Error

La existencia de bugs, vulnerabilidades, exploits, errores de programación, fallas de oráculos, errores de interfaz o ejecución inesperada de smart contracts podrá dar lugar a revisión, restitución, indemnización, nulidad, corrección o medidas judiciales cuando afecte derechos, consentimiento, patrimonio, consumidores o terceros.

No toda pérdida derivada de un smart contract implicará responsabilidad. La responsabilidad dependerá de dolo, negligencia, ocultamiento, deberes asumidos, disclosure, control efectivo, auditorías realizadas y conducta de las partes.

Artículo 674. Cláusulas Contrarias a Derechos Fundamentales

Serán nulas o inoponibles las cláusulas, condiciones, smart contracts o ejecuciones programables que pretendan excluir derechos fundamentales, debido proceso, tutela judicial efectiva, protección del consumidor, privacidad, prohibición de discriminación, acceso a la justicia o responsabilidad por fraude.

SECCIÓN IV — JURISDICCIÓN Y DERECHO APLICABLE

Artículo 675. Jurisdicción en Entornos Descentralizados

La jurisdicción aplicable a relaciones jurídicas digitales podrá determinarse según:

a) Elección válida de las partes.
b) Domicilio o residencia de partes relevantes.
c) Lugar de prestación del servicio.
d) Ubicación del activo subyacente.
e) Jurisdicción del emisor o plataforma.
f) Lugar de administración efectiva.
g) Mercado al que se dirige la oferta.
h) Lugar donde se produce daño relevante.
i) Registro aplicable.
j) Conexión sustancial con Costa Rica.

La mera accesibilidad global de un protocolo o sitio web no determinará por sí sola jurisdicción costarricense sin conexión sustancial.

Artículo 676. DAOs y Jurisdicción

En controversias relacionadas con DAOs, la jurisdicción podrá determinarse según:

a) Registro DAO.
b) Wrapper legal.
c) Lugar de administración efectiva.
d) Elección de foro en reglas de gobernanza.
e) Ubicación de representantes o signatarios.
f) Actividad económica dirigida a Costa Rica.
g) Tokenización de activos costarricenses.
h) Prestación de servicios regulados en Costa Rica.
i) Lugar donde se produjo daño relevante.

La participación de una persona costarricense en una DAO global no bastará por sí sola para someter toda la DAO a jurisdicción costarricense.

Artículo 677. Conflictos Transfronterizos

Los conflictos transfronterizos sobre activos digitales, DAOs, smart contracts, tokenización, VASP, stablecoins, mercados digitales o infraestructura descentralizada deberán resolverse atendiendo a buena fe, elección de ley, protección de usuarios, prevención de fraude, conexión sustancial, orden público costarricense y estándares internacionales aplicables.

Artículo 678. Elección de Ley Aplicable

Las partes podrán elegir ley aplicable y foro competente para resolver controversias digitales, incluyendo arbitraje, mediación, tribunales especializados o mecanismos on-chain, siempre que dicha elección sea válida, clara, accesible y no vulnere derechos irrenunciables, consumidores, usuarios minoristas o normas de orden público.

SECCIÓN V — ARBITRAJE DIGITAL Y RESOLUCIÓN WEB3

Artículo 679. Validez del Arbitraje Digital

Se reconoce la validez del arbitraje digital para controversias relacionadas con activos digitales, smart contracts, DAOs, tokenización, RWA, mercados digitales, propiedad intelectual tokenizada, infraestructura Web3, pagos blockchain, stablecoins y demás relaciones jurídicas digitales.

El arbitraje podrá realizarse de forma presencial, remota, híbrida, documentaria, acelerada, técnica, on-chain o mediante plataformas especializadas, respetando igualdad de partes, derecho de defensa, independencia, imparcialidad y debido proceso.

Artículo 680. Centros y Tribunales Arbitrales Especializados en Web3

Podrán crearse centros, cámaras, paneles o tribunales arbitrales especializados en Web3, blockchain, activos digitales, smart contracts, DAOs, tokenización, ciberseguridad, IA, propiedad digital y evidencia criptográfica.

Los árbitros y peritos deberán contar con idoneidad técnica y jurídica suficiente para comprender la materia sometida a decisión.

Artículo 681. Arbitraje On-Chain

Las partes podrán pactar arbitraje on-chain o mecanismos de resolución descentralizada de controversias, incluyendo jurados digitales, votación especializada, smart contract escrow, mecanismos de oracle dispute resolution, multisig adjudication o plataformas de justicia descentralizada.

Estos mecanismos serán válidos cuando garanticen:

a) Consentimiento claro.
b) Reglas accesibles.
c) Independencia razonable.
d) Derecho de defensa.
e) Presentación de prueba.
f) Imparcialidad.
g) Posibilidad de revisión o control cuando afecte derechos esenciales.
h) Compatibilidad con orden público.

Artículo 682. Mediación Tecnológica

Las controversias digitales podrán someterse a mediación tecnológica, negociación asistida por plataformas, resolución temprana, peritaje neutral, evaluación técnica independiente o mecanismos comunitarios de solución de disputas.

SECCIÓN VI — EJECUCIÓN Y ENFORCEMENT

Artículo 683. Ejecución de Acuerdos Digitales

Los acuerdos digitales, transacciones, smart contracts, laudos, resoluciones arbitrales, settlements, decisiones DAO o acuerdos de mediación podrán ejecutarse conforme a la ley cuando sean válidos, verificables y no contrarios al orden público.

La ejecución podrá incluir transferencia de activos, liberación de garantías, actualización registral, restitución, bloqueo específico, corrección de registros, compensación o ejecución sobre colateral, siempre con garantías aplicables.

Artículo 684. Reconocimiento de Laudos Digitales

Los laudos arbitrales dictados en controversias digitales serán reconocidos y ejecutables conforme al régimen arbitral aplicable, tratados internacionales y normas costarricenses, siempre que se respete debido proceso, competencia arbitral, notificación, imparcialidad y orden público.

La emisión, firma o conservación digital del laudo no afectará su validez si permite verificar autenticidad e integridad.

Artículo 685. Enforcement Compatible con Derechos Fundamentales

Toda ejecución sobre activos digitales, wallets, tokens, smart contracts, DAOs, mercados o registros deberá respetar proporcionalidad, individualización, protección de terceros de buena fe, privacidad, debido proceso y tutela judicial efectiva.

Quedan prohibidas ejecuciones masivas, indiscriminadas o técnicamente desproporcionadas que afecten usuarios inocentes o infraestructura neutral.

SECCIÓN VII — PROTECCIÓN DE DERECHOS FUNDAMENTALES

Artículo 686. Límites del "Code is Law"

El principio "code is law" no tendrá valor absoluto dentro del ordenamiento costarricense.

La ejecución de código, smart contracts o protocolos no podrá prevalecer sobre derechos fundamentales, protección del consumidor, prohibición de fraude, debido proceso, propiedad legítima, orden público, buena fe, equidad contractual o tutela judicial efectiva.

Artículo 687. Protección del Debido Proceso

Toda persona afectada por decisiones automatizadas, ejecuciones programables, smart contracts, governance attacks, liquidaciones, bloqueos, sanciones, slashing, exclusiones o votaciones DAO tendrá derecho a los mecanismos de defensa que correspondan según la naturaleza de la relación, el riesgo asumido y la ley aplicable.

Artículo 688. Protección de Usuarios Vulnerables

Cuando existan consumidores, usuarios principiantes, inversionistas minoristas o personas en situación de vulnerabilidad, las cláusulas de arbitraje, jurisdicción, smart contracts, renuncias o mecanismos on-chain deberán interpretarse conforme a protección reforzada, transparencia y consentimiento informado.

SECCIÓN VIII — CLÁUSULAS FINALES

Artículo 689. Cláusula de Compatibilidad Tecnológica

Toda norma procesal, contractual, probatoria o arbitral deberá interpretarse de forma compatible con blockchain, smart contracts, identidad soberana, firmas criptográficas, DAOs, evidencia on-chain y activos digitales, siempre que se respeten derechos fundamentales y garantías procesales.

Artículo 690. Cláusula de Evolución Digital

La IID, el Poder Judicial, centros arbitrales, universidades y colegios profesionales podrán emitir guías, protocolos, estándares y formación especializada para valoración de evidencia criptográfica, resolución de controversias Web3, arbitraje digital y ejecución de smart contracts.

Artículo 691. Cláusula de Soberanía Jurídica Digital

Costa Rica ejercerá soberanía jurídica digital para reconocer relaciones Web3, resolver controversias digitales, proteger derechos fundamentales, admitir evidencia criptográfica y desarrollar arbitraje especializado sin someterse automáticamente a modelos extranjeros incompatibles con su Constitución, orden público y principios de libertad digital.

CAPÍTULO XXII — COOPERACIÓN INTERNACIONAL, INTEROPERABILIDAD GLOBAL Y POSICIONAMIENTO GEOESTRATÉGICO DE COSTA RICA

SECCIÓN I — PRINCIPIOS DE SOBERANÍA REGULATORIA INTERNACIONAL

Artículo 692. Soberanía Regulatoria Digital Internacional

Costa Rica ejercerá su potestad regulatoria en materia de activos digitales, blockchain, inteligencia artificial, identidad soberana, DeFi, tokenización y mercados digitales dentro del marco de la Constitución Política, los tratados vigentes y el ordenamiento jurídico nacional.

La IID podrá celebrar memorandos técnicos, mecanismos de cooperación, reconocimiento o interoperabilidad regulatoria dentro de sus competencias, pero dichos instrumentos no podrán transferir competencias constitucionales a autoridades extranjeras, crear obligaciones reservadas a tratado o modificar la jerarquía normativa nacional.

Artículo 693. Cooperación Internacional Garantista

El Estado podrá cooperar con organismos internacionales, autoridades extranjeras, reguladores, agencias de supervisión, tribunales, centros arbitrales y entidades técnicas para prevenir fraude, lavado de dinero, financiamiento ilícito, cibercrimen, manipulación de mercado, abuso financiero y riesgos sistémicos.

Toda cooperación deberá respetar legalidad, proporcionalidad, debido proceso, protección de datos, orden público costarricense y derechos digitales.

Artículo 694. No Subordinación Automática a Modelos Extranjeros

Ningún estándar, recomendación, guía, marco extranjero, política de organismo internacional o regulación comparada será incorporada automáticamente al ordenamiento costarricense si contradice derechos fundamentales digitales, autocustodia, privacidad criptográfica, neutralidad tecnológica o soberanía financiera.

Su adopción requerirá análisis de compatibilidad constitucional, consulta pública y evaluación técnica.

SECCIÓN II — COOPERACIÓN AML/CFT Y ESTÁNDARES INTERNACIONALES

Artículo 695. Implementación Garantista de Estándares AML/CFT

Costa Rica implementará estándares internacionales de prevención de lavado de dinero, financiamiento del terrorismo y financiamiento de proliferación en materia de activos digitales bajo un enfoque basado en riesgo, proporcionalidad, neutralidad tecnológica y respeto a derechos fundamentales.

Las obligaciones deberán dirigirse prioritariamente a sujetos con control efectivo, custodia, intermediación, administración de activos de terceros, emisión, operación de mercados o actividad profesional regulada.

Artículo 696. Travel Rule Compatible con Autocustodia

La aplicación de reglas internacionales de transferencia de información deberá concentrarse en VASP, custodios, bancos digitales, exchanges, plataformas y sujetos regulados.

Las transferencias entre wallets no custodiales no serán tratadas automáticamente como transferencias reguladas, salvo que exista intermediación profesional, actividad empresarial organizada, custodia de terceros o indicios verificables de ilicitud.

Artículo 697. Cooperación en Investigaciones Transfronterizas

La cooperación en investigaciones sobre activos digitales deberá basarse en solicitudes individualizadas, fundamentadas, proporcionales y sujetas a control legal.

No se permitirá intercambio masivo, indiscriminado o preventivo de datos financieros, identidades digitales, wallets, transacciones, biometría o credenciales sin base legal suficiente.

Artículo 698. Protección de Datos en Cooperación Internacional

Toda transferencia internacional de datos vinculada a activos digitales, identidad digital, wallets, usuarios, transacciones, registros, credenciales o investigaciones deberá cumplir estándares de protección de datos, minimización, finalidad específica, seguridad y trazabilidad.

SECCIÓN III — INTEROPERABILIDAD REGULATORIA GLOBAL

Artículo 699. Pasarelas Regulatorias Internacionales

La IID podrá establecer pasarelas regulatorias, memorandos de entendimiento, acuerdos de cooperación, sandboxes transfronterizos y mecanismos de reconocimiento técnico con autoridades extranjeras.

Estos instrumentos podrán facilitar:

a) Licenciamiento transfronterizo.
b) Supervisión coordinada.
c) Intercambio de información proporcional.
d) Protección de usuarios.
e) Reconocimiento de estándares.
f) Innovación internacional.
g) Testing regulatorio.
h) Tokenización transfronteriza.
i) Mercados secundarios interoperables.
j) Compliance criptográfico.

Artículo 700. Reconocimiento de Licencias Extranjeras

La IID podrá reconocer total o parcialmente licencias, autorizaciones o registros emitidos por jurisdicciones extranjeras cuando estas mantengan estándares equivalentes de supervisión, protección al usuario, AML/CFT, ciberseguridad, transparencia y Estado de Derecho.

El reconocimiento no será automático y podrá estar sujeto a condiciones, registro local, supervisión limitada, obligaciones de información o representación en Costa Rica.

Artículo 701. Reconocimiento de Estándares Técnicos Internacionales

La IID podrá reconocer estándares internacionales en materia de:

a) Blockchain.
b) Ciberseguridad.
c) Criptografía post-cuántica.
d) Identidad digital.
e) ZKP.
f) Proof of reserves.
g) Auditoría de smart contracts.
h) Tokenización RWA.
i) Stablecoins.
j) Custodia digital.
k) Compliance criptográfico.
l) Interoperabilidad de mercados.

SECCIÓN IV — RECONOCIMIENTO TRANSFRONTERIZO DE ACTIVOS Y MERCADOS

Artículo 702. Reconocimiento de Activos Digitales Extranjeros

Los activos digitales emitidos, tokenizados, registrados o negociados en jurisdicciones extranjeras podrán ser reconocidos en Costa Rica conforme a su naturaleza jurídica, nivel de riesgo, disclosure, supervisión aplicable y compatibilidad con la ley costarricense.

La IID podrá requerir información adicional cuando dichos activos se ofrezcan al público costarricense o se negocien en mercados regulados nacionales.

Artículo 703. Tokenización Transfronteriza

Costa Rica podrá reconocer estructuras de tokenización extranjeras cuando exista claridad sobre el activo subyacente, titularidad, derechos del token holder, jurisdicción, custodia, auditoría, gravámenes, riesgos y mecanismos de ejecución.

Los activos costarricenses tokenizados desde el extranjero deberán cumplir las normas nacionales aplicables cuando el subyacente esté ubicado o registrado en Costa Rica.

Artículo 704. Mercados Digitales Internacionales

La IID podrá permitir acceso a mercados digitales internacionales, plataformas extranjeras, bolsas de activos digitales, ATS Web3, stablecoin issuers o infraestructura global, siempre que existan estándares mínimos de transparencia, protección de usuarios, AML/CFT, ciberseguridad y cooperación.

SECCIÓN V — POSICIONAMIENTO DE COSTA RICA COMO HUB WEB3 GLOBAL

Artículo 705. Estrategia Nacional de Posicionamiento Web3

El Estado adoptará una estrategia nacional para posicionar a Costa Rica como jurisdicción líder en Web3, blockchain, activos digitales, tokenización, identidad soberana, IA garantista, ciberseguridad, criptografía post-cuántica, compliance criptográfico, arbitraje digital y economía descentralizada.

Esta estrategia deberá involucrar sector público, sector privado, universidades, comunidades técnicas, zonas francas tecnológicas, inversionistas, embajadas y organismos internacionales.

Artículo 706. Marca País Digital

El Estado podrá desarrollar una estrategia de Marca País Digital para promover a Costa Rica como:

a) Democracia digital garantista.
b) Hub Web3 legítimo.
c) Jurisdicción de tokenización segura.
d) Centro de arbitraje digital.
e) Ecosistema de IA responsable.
f) Destino de talento tecnológico.
g) País de identidad soberana.
h) Centro de ciberseguridad y post-cuántica.
i) Jurisdicción de libertad financiera con cumplimiento.

Artículo 707. Atracción de Inversión Web3

El Estado promoverá inversión extranjera directa en infraestructura Web3, tokenización, mercados digitales, bancos blockchain-native, IA, ciberseguridad, centros de datos, validadores, ZKP, post-cuántica, software open-source, educación y exportación de servicios digitales.

Artículo 708. Competencia Regional Estratégica

La política pública deberá evaluar periódicamente la competitividad de Costa Rica frente a jurisdicciones Web3 relevantes, incluyendo El Salvador, Suiza, Liechtenstein, Singapur, Hong Kong, Dubái, Abu Dhabi, Wyoming, Delaware, Panamá y otros hubs emergentes.

La evaluación deberá considerar costos regulatorios, incentivos fiscales, tiempo de licenciamiento, seguridad jurídica, talento, infraestructura, derechos digitales, reputación democrática y acceso internacional.

SECCIÓN VI — TALENTO, MOVILIDAD E INNOVACIÓN TRANSFRONTERIZA

Artículo 709. Visas y Residencias Tecnológicas

Costa Rica podrá establecer categorías migratorias especiales para fundadores, desarrolladores, investigadores, criptógrafos, expertos en IA, auditores de smart contracts, especialistas en ciberseguridad, operadores de infraestructura, inversionistas Web3 y talento estratégico.

Artículo 710. Reconocimiento Internacional de Certificaciones

El Estado podrá reconocer certificaciones internacionales en blockchain, ciberseguridad, IA, criptografía, auditoría de smart contracts, protección de datos, AML/CFT digital y tecnologías emergentes, conforme a estándares de calidad e idoneidad.

Artículo 711. Alianzas Académicas y Tecnológicas Internacionales

Costa Rica promoverá alianzas con universidades, centros de investigación, laboratorios, organismos técnicos, comunidades open-source y hubs tecnológicos internacionales para fortalecer investigación, formación, certificación, desarrollo de infraestructura y transferencia de conocimiento.

SECCIÓN VII — PROTECCIÓN FRENTE A IMPOSICIONES INCOMPATIBLES CON EL ORDEN CONSTITUCIONAL

Artículo 712. Control de Compatibilidad con el Orden Constitucional y los Derechos

La adopción interna de estándares, acuerdos, obligaciones o recomendaciones internacionales en materia de activos digitales, identidad digital, inteligencia artificial, AML/CFT, ciberseguridad o blockchain deberá realizarse de conformidad con la Constitución Política, los tratados vigentes, los derechos fundamentales y los procedimientos de incorporación que correspondan.

Las autoridades deberán procurar compatibilidad con autocustodia, privacidad financiera, identidad soberana, neutralidad tecnológica, debido proceso digital, libertad financiera, protección de software libre y prohibición de vigilancia masiva, sin desconocer obligaciones internacionales válidamente incorporadas al ordenamiento.

El intercambio transfronterizo de información no habilitará por sí mismo acceso a documentos privados, comunicaciones o datos protegidos fuera de los supuestos autorizados por la Constitución, la ley y los instrumentos internacionales aplicables.

Artículo 713. Prohibición de Importar Vigilancia Masiva

Queda prohibido adoptar, implementar o reconocer mecanismos internacionales que obliguen a vigilancia masiva, identificación universal de wallets, debilitamiento criptográfico, escaneo indiscriminado, scoring financiero global o intercambio preventivo de datos sin sospecha individualizada.

Artículo 714. Defensa Internacional de la Autocustodia

Costa Rica promoverá en foros internacionales el reconocimiento de la autocustodia como derecho patrimonial digital legítimo, compatible con prevención de delitos financieros mediante modelos proporcionales, compliance criptográfico y pruebas selectivas.

SECCIÓN VIII — DIPLOMACIA TECNOLÓGICA Y SOBERANÍA DIGITAL INTERNACIONAL

Artículo 715. Diplomacia Tecnológica

El Estado desarrollará una política de diplomacia tecnológica orientada a posicionar a Costa Rica en discusiones globales sobre blockchain, IA, activos digitales, identidad digital, ciberseguridad, criptografía post-cuántica, privacidad y economía descentralizada.

Artículo 716. Participación en Foros Internacionales

Costa Rica promoverá participación activa en foros internacionales relacionados con activos digitales, blockchain, IA, ciberseguridad, estándares técnicos, protección de datos, gobernanza de internet, interoperabilidad financiera, AML/CFT y derechos digitales.

Artículo 717. Cooperación Sur-Sur y Liderazgo Latinoamericano

Costa Rica podrá liderar iniciativas regionales de cooperación Web3 en América Latina, incluyendo interoperabilidad regulatoria, educación, tokenización, pagos digitales, identidad soberana, arbitraje digital, ciberseguridad e innovación pública.

SECCIÓN IX — CLÁUSULAS FINALES DE POSICIONAMIENTO GLOBAL

Artículo 718. Cláusula de Apertura Global con Soberanía

Toda política internacional sobre activos digitales deberá equilibrar apertura global, cooperación regulatoria, atracción de inversión, protección del usuario, seguridad jurídica, soberanía financiera y derechos fundamentales digitales.

Artículo 719. Cláusula de Competitividad Geoestratégica

La IID y las autoridades competentes deberán evaluar permanentemente el posicionamiento de Costa Rica frente a hubs globales y proponer reformas para mantener competitividad, legitimidad y liderazgo tecnológico.

Artículo 720. Cláusula de Liderazgo Democrático Web3

Costa Rica orientará su política internacional a consolidarse como una democracia digital líder: abierta a la innovación, compatible con estándares internacionales, respetuosa de derechos humanos, defensora de autocustodia, enemiga de la vigilancia masiva y promotora de soberanía digital.

CAPÍTULO XXIII — EDUCACIÓN, TALENTO, INVESTIGACIÓN Y TRANSFORMACIÓN NACIONAL DIGITAL

SECCIÓN I — PRINCIPIOS DE TRANSFORMACIÓN NACIONAL

Artículo 721. Educación como Infraestructura de Soberanía

El Estado reconocerá la educación tecnológica, financiera digital, criptográfica, algorítmica y computacional como infraestructura estratégica de soberanía nacional.

La formación en blockchain, activos digitales, inteligencia artificial, ciberseguridad, privacidad, programación, datos, criptografía, tokenización y economía digital será promovida como parte esencial del desarrollo nacional.

Artículo 722. Alfabetización Digital Nacional

El Estado impulsará una política nacional de alfabetización digital soberana orientada a que la ciudadanía comprenda:

a) Derechos digitales.
b) Privacidad.
c) Identidad digital soberana.
d) Autocustodia.
e) Seguridad de wallets.
f) Riesgos de fraudes digitales.
g) IA y manipulación algorítmica.
h) Blockchain y activos digitales.
i) Protección de datos.
j) Ciberseguridad básica.
k) Desinformación digital.
l) Uso responsable de tecnología.

Artículo 723. Derecho a Educación Tecnológica

Toda persona tendrá derecho a acceder progresivamente a educación tecnológica pertinente, actualizada, inclusiva y orientada a la participación segura en la economía digital.

El Estado deberá promover acceso a formación en zonas urbanas, rurales, costeras, fronterizas, indígenas y de menor desarrollo relativo.

SECCIÓN II — EDUCACIÓN PÚBLICA, TÉCNICA Y UNIVERSITARIA

Artículo 724. Blockchain en Educación Superior

El Estado promoverá la incorporación de blockchain, activos digitales, tokenización, smart contracts, DeFi, identidad digital, gobernanza descentralizada y regulación tecnológica en programas universitarios, técnicos y de educación continua.

Las universidades públicas y privadas podrán desarrollar carreras, especializaciones, certificaciones, laboratorios y clínicas jurídicas-tecnológicas en estas materias.

Artículo 725. Criptografía, Programación y Seguridad

El Estado promoverá formación en criptografía aplicada, programación, seguridad de software, auditoría de smart contracts, desarrollo de wallets, sistemas distribuidos, redes peer-to-peer, seguridad de llaves y arquitectura blockchain.

Artículo 726. Inteligencia Artificial, ZKP y Criptografía Post-Cuántica

Los programas de educación superior, técnica e investigación deberán promover formación en:

a) Inteligencia artificial.
b) Auditoría algorítmica.
c) Zero Knowledge Proofs.
d) Criptografía post-cuántica.
e) Computación distribuida.
f) Privacidad por diseño.
g) Seguridad de modelos.
h) IA descentralizada.

i) Verificación formal.
j) Ética tecnológica.

Artículo 727. Formación Técnica Nacional

El Estado promoverá programas técnicos de rápida inserción laboral en:

a) Desarrollo blockchain.
b) Ciberseguridad.
c) Auditoría de smart contracts.
d) Análisis on-chain.
e) Operación de nodos y validadores.
f) Soporte de wallets.
g) Compliance criptográfico.
h) IA aplicada.
i) Infraestructura cloud.
j) Administración de sistemas Web3.

SECCIÓN III — FORMACIÓN INSTITUCIONAL DEL ESTADO

Artículo 728. Capacitación Judicial

El Poder Judicial, en el marco de su autonomía y conforme a los mecanismos institucionales que determine, podrá desarrollar programas de capacitación en evidencia on-chain, activos digitales, blockchain, inteligencia artificial, criptografía, smart contracts, DAOs, ciberseguridad y tecnologías emergentes cuando resulte pertinente para el ejercicio de sus funciones.

El MICITT y la IID podrán ofrecer cooperación técnica, materiales y programas de formación a solicitud de las autoridades judiciales competentes, sin interferir en su organización, funciones jurisdiccionales ni independencia.

Artículo 729. Formación de Reguladores

La IID y demás autoridades competentes deberán contar con programas permanentes de formación técnica en blockchain, DeFi, tokenización, stablecoins, VASP, compliance criptográfico, ZKP, ciberseguridad, IA y regulación comparada.

Artículo 730. Capacitación de Fuerzas Públicas e Investigadores

Las autoridades policiales, fiscales, administrativas y de investigación deberán recibir formación en investigación digital, trazabilidad on-chain, preservación de evidencia, delitos financieros digitales, protección de datos, límites constitucionales y no criminalización de autocustodia.

Artículo 731. Transformación Digital Estatal

El Estado impulsará formación de funcionarios públicos en gobierno digital, blockchain anticorrupción, datos abiertos, ciberseguridad, identidad soberana, IA responsable, smart contracts estatales, protección de datos e interoperabilidad.

SECCIÓN IV — INVESTIGACIÓN Y DESARROLLO

Artículo 732. Centros Nacionales de Investigación Digital

El Estado podrá promover centros nacionales o alianzas público-privadas de investigación en:

a) Blockchain.
b) Inteligencia artificial.

c) Criptografía.
d) Ciberseguridad.
e) Computación post-cuántica.
f) ZKP.
g) Tokenización.
h) Identidad soberana.
i) DeFi.
j) Gobernanza digital.
k) Sistemas electorales verificables.
l) Registro Público blockchain.

Artículo 733. Incentivos a Investigación

El Estado podrá otorgar incentivos, fondos, becas, grants, créditos fiscales, compras públicas innovadoras, sandboxes académicos y apoyo institucional a proyectos de investigación relacionados con tecnologías descentralizadas, IA, ciberseguridad y computación avanzada.

Artículo 734. Open Source y Soberanía Tecnológica

El Estado promoverá el desarrollo, auditoría y adopción de software open-source en infraestructura pública digital, siempre que sea seguro, auditable, interoperable y sostenible.

Podrán impulsarse repositorios públicos, grants de software libre, auditorías comunitarias, hackathons, laboratorios de código abierto y colaboración internacional.

Artículo 735. Investigación Post-Cuántica

Costa Rica impulsará investigación, formación y adopción gradual de criptografía post-cuántica, criptoagilidad, seguridad de llaves, migración criptográfica y protección contra amenazas futuras.

SECCIÓN V — INCLUSIÓN Y RECONVERSIÓN ECONÓMICA

Artículo 736. Inclusión Financiera Digital

El Estado promoverá el uso de tecnologías digitales descentralizadas para ampliar inclusión financiera, pagos accesibles, remesas de bajo costo, ahorro digital, educación financiera, acceso a mercados globales y participación económica de poblaciones históricamente excluidas.

Artículo 737. Reconversión Laboral Tecnológica

El Estado impulsará programas de reconversión laboral para trabajadores afectados por automatización, IA, digitalización, transformación financiera o cambios productivos.

Los programas podrán incluir formación en programación, análisis de datos, ciberseguridad, soporte tecnológico, compliance digital, marketing Web3, diseño, educación digital y servicios profesionales tecnológicos.

Artículo 738. Emprendimiento Web3

El Estado fomentará emprendimientos Web3 mediante incubadoras, aceleradoras, sandboxes, fondos semilla, mentorías, educación empresarial, acceso a inversión, simplificación de trámites y conexión con mercados internacionales.

Artículo 739. Acceso Regional, Rural e Indígena

La estrategia de transformación digital deberá incluir acceso regional, rural, costero, fronterizo e indígena a conectividad, educación tecnológica, herramientas digitales, capacitación, emprendimiento y protección de derechos digitales.

Toda política deberá respetar diversidad cultural, lenguas, autonomía comunitaria y pertinencia local.

SECCIÓN VI — TALENTO INTERNACIONAL Y COMPETITIVIDAD

Artículo 740. Atracción de Talento Global

Costa Rica podrá implementar programas para atraer talento internacional en blockchain, IA, criptografía, ciberseguridad, tokenización, ZKP, post-cuántica, DeFi, arbitraje digital y economía digital.

Estos programas podrán incluir facilidades migratorias, incentivos, visas tecnológicas, reconocimiento de certificaciones y vinculación con empresas nacionales.

Artículo 741. Certificaciones y Competencias

El Estado podrá promover marcos de certificación nacional e internacional en competencias Web3, IA, ciberseguridad, blockchain, auditoría de smart contracts, compliance criptográfico, identidad digital y protección de datos.

Artículo 742. Costa Rica como Hub Educativo Web3

Costa Rica promoverá su posicionamiento como hub regional de educación Web3, IA, ciberseguridad, blockchain, identidad soberana, regulación tecnológica y arbitraje digital.

Podrán desarrollarse programas bilingües, certificaciones internacionales, congresos, investigación aplicada, alianzas universitarias y formación ejecutiva.

SECCIÓN VII — CLÁUSULAS FINALES

Artículo 743. Cláusula de Soberanía del Conocimiento

Toda política pública relacionada con tecnología deberá promover la capacidad nacional de comprender, auditar, desarrollar, adaptar y gobernar infraestructura digital crítica.

Artículo 744. Cláusula Anti Dependencia Tecnológica

El Estado deberá evitar modelos educativos, tecnológicos o contractuales que generen dependencia estructural de proveedores, plataformas, software cerrado, conocimiento extranjero no transferible o infraestructura no auditable.

Artículo 745. Cláusula de Evolución Educativa Permanente

Los programas educativos, técnicos, regulatorios y judiciales relacionados con tecnologías emergentes deberán actualizarse periódicamente conforme al avance de blockchain, inteligencia artificial, criptografía, computación cuántica, ciberseguridad, mercados digitales y derechos digitales.

La actualización se realizará sin perjuicio de la autonomía constitucional universitaria y de las competencias legales de las autoridades educativas y judiciales. En el caso de universidades públicas, las disposiciones de esta ley se entenderán como objetivos de cooperación y política pública, no como sustitución de sus órganos de gobierno académico.

CAPÍTULO XXIV — GARANTÍAS DIGITALES, DERECHOS POST-MORTEM Y ARMONIZACIÓN DEL ORDENAMIENTO JURÍDICO

SECCIÓN I — DESARROLLO LEGISLATIVO DE GARANTÍAS DIGITALES

Artículo 746. Garantías digitales y relación con la Constitución Política

Los derechos y garantías digitales reconocidos por esta ley desarrollan, en el entorno tecnológico, los derechos de dignidad, intimidad, propiedad, libertad de expresión, libertad contractual, debido proceso, igualdad y tutela efectiva reconocidos por el ordenamiento constitucional.

La incorporación de nuevas disposiciones al texto de la Constitución Política requerirá el procedimiento de reforma parcial previsto en el artículo 195 constitucional y se tramitará mediante expediente complementario.

Artículo 747. Garantía legal de identidad digital soberana

Toda persona tiene derecho al control, portabilidad, minimización y protección de su identidad digital, credenciales y atributos verificables. Ningún sistema público o privado podrá convertir la identidad digital en mecanismo de vigilancia o exclusión generalizada.

Artículo 748. Garantía legal de autocustodia

La autocustodia de activos digitales propios se reconoce como ejercicio de propiedad y autonomía patrimonial. No podrá imponerse custodia de terceros como regla general, sin perjuicio de medidas individualizadas previstas por ley.

Artículo 749. Libertad financiera digital

Toda persona podrá participar en actividades digitales lícitas, utilizar infraestructura abierta y transferir valor directamente, sin discriminación tecnológica arbitraria y sin perjuicio de las obligaciones aplicables a intermediarios profesionales.

Artículo 750. Protección reforzada de la criptografía

El uso legítimo de criptografía fuerte constituye una herramienta de privacidad, seguridad, propiedad e identidad. Se prohíben puertas traseras y debilitamiento general del cifrado; las medidas investigativas deberán ser individualizadas y sujetas a ley y debido proceso.

Artículo 751. Prohibición legal de vigilancia masiva

Queda prohibida la vigilancia digital masiva, indiscriminada o permanente de la población. Las medidas de vigilancia legítimas deberán responder a una finalidad legal, ser necesarias, individualizadas, proporcionales, temporales y sujetas a control competente.

Artículo 752. Límites a monedas digitales estatales de control social

Queda prohibida la imposición de una moneda digital estatal minorista diseñada para vigilancia masiva, scoring social, expiración arbitraria, condicionamiento político o restricción conductual generalizada. Esta norma no impide innovación monetaria o de liquidación compatible con derechos fundamentales y con las competencias del Banco Central de Costa Rica.

Artículo 753. Neutralidad tecnológica

Las autoridades deberán regular funciones, riesgos y control efectivo y no favorecer o perjudicar tecnologías, redes o modelos lícitos sin justificación objetiva y proporcional.

Artículo 754. Protección del software libre y código abierto

La creación, publicación, estudio, auditoría, modificación y distribución de código abierto y software libre lícito se reconoce como actividad protegida por las libertades de expresión, investigación, creación e innovación. La mera publicación de código neutral no constituye por sí misma actividad financiera ni genera responsabilidad por actos independientes de terceros; ello no excluye responsabilidad por fraude, control operativo o participación dolosa en conductas ilícitas.

Artículo 755. Protección de propiedad digital

La forma digital o tokenizada de un bien o derecho no disminuye su protección jurídica. Los activos digitales lícitamente adquiridos integran el patrimonio de su titular y están sujetos a propiedad, transmisión, garantía, sucesión y tutela efectiva según su naturaleza.

SECCIÓN II — GARANTÍAS DIGITALES REFORZADAS

Artículo 756. Habeas data y autodeterminación informativa digital

Toda persona podrá conocer, acceder, rectificar, portar, limitar, oponerse y exigir supresión cuando proceda respecto de sus datos digitales, conforme al régimen de protección de datos y las garantías reforzadas de esta ley.

Artículo 757. Tutela judicial efectiva digital

Los tribunales deberán garantizar tutela efectiva frente a afectaciones de identidad, propiedad, datos, activos digitales, decisiones automatizadas, autocustodia, criptografía y demás derechos reconocidos por esta ley. La ausencia de una categoría tecnológica específica no podrá utilizarse para denegar justicia.

Artículo 758. Debido proceso algorítmico

Ninguna decisión automatizada de alto impacto que afecte derechos fundamentales podrá producir efectos definitivos sin información suficiente sobre su fundamento, posibilidad real de revisión humana e impugnación, salvo excepciones legales compatibles con la Constitución.

Artículo 759. Derecho a explicación y trazabilidad proporcional

Las personas afectadas por sistemas automatizados de alto impacto tendrán derecho a conocer la finalidad, factores relevantes, autoridad o responsable, vías de revisión y elementos suficientes para controvertir la decisión, sin exigir divulgación de secretos que no resulten necesarios para ejercer defensa efectiva.

SECCIÓN III — ARMONIZACIÓN DEL ORDENAMIENTO JURÍDICO

Artículo 760. Armonización con el Código Civil

El Poder Ejecutivo, la IID y las autoridades competentes deberán proponer reformas al Código Civil para reconocer:

a) Propiedad digital.
b) Activos digitales como bienes patrimoniales.
c) Sucesión de activos digitales.
d) Contratos inteligentes.
e) Firma criptográfica.
f) Representación tokenizada de derechos.
g) Custodia digital.
h) Responsabilidad por pérdida o apropiación de activos digitales.

Artículo 761. Armonización Mercantil

Deberán armonizarse las normas mercantiles para permitir:

a) Sociedades con registros digitales.
b) Participaciones tokenizadas.
c) Libros societarios blockchain.
d) DAOs con personalidad jurídica.
e) Títulos y valores tokenizados.
f) Smart contracts comerciales.
g) Comercio transfronterizo digital.
h) Facturación y financiamiento tokenizado.

Artículo 762. Coordinación Especial con la Ley Reguladora del Mercado de Valores

La Ley Reguladora del Mercado de Valores, N.° 7732, continuará aplicándose a los valores, emisores, ofertas públicas, intermediarios y mercados comprendidos en su ámbito material, salvo las reglas especiales que esta ley establezca expresamente para activos digitales nativos y mercados digitales bajo competencia de la IID.

La utilización de blockchain, tokenización o registros distribuidos no excluirá por sí sola la aplicación de la Ley N.° 7732 cuando el activo represente sustancialmente un valor tradicional o una oferta pública sometida a dicho régimen. En productos híbridos, la IID y SUGEVAL deberán aplicar un procedimiento de determinación de perímetro basado en sustancia económica, derechos conferidos, forma de colocación, control efectivo y riesgos para inversionistas.

El Poder Ejecutivo, la IID, SUGEVAL y CONASSIF deberán proponer, dentro de los doce meses siguientes a la publicación de esta ley, las reformas reglamentarias y legales de precisión necesarias para eliminar duplicidades, sin suspender la aplicación inmediata de las reglas de coordinación previstas en este artículo.

Artículo 763. Coordinación Bancaria, Monetaria y AML/CFT

Las competencias del Banco Central de Costa Rica, CONASSIF, SUGEF y demás autoridades financieras se preservan en materia monetaria, cambiaria, prudencial, intermediación financiera, estabilidad y sistemas de pago, conforme a la legislación vigente.

Los proveedores de servicios de activos virtuales sujetos a inscripción, supervisión u obligaciones AML/CFT bajo la Ley N.° 7786 continuarán cumpliendo ese régimen ante las autoridades competentes. La autorización sectorial o registro ante la IID no sustituirá ni duplicará las obligaciones AML/CFT establecidas por ley.

La IID y SUGEF deberán implementar interoperabilidad registral, intercambio de información legalmente permitido, coordinación de supervisión y mecanismos de ventanilla única cuando ello reduzca cargas duplicadas. El acceso a información reservada se regirá exclusivamente por las habilitaciones constitucionales y legales aplicables.

La IID conservará la supervisión sectorial especializada sobre actividades Web3 comprendidas en su perímetro, mientras SUGEF mantendrá las competencias AML/CFT y prudenciales que le atribuya el ordenamiento. Ninguna autoridad podrá utilizar la coordinación para ampliar sus competencias más allá de la ley.

Artículo 764. Coordinación Registral y Notarial

Las funcionalidades de fe pública criptográfica, tokenización registral, smart contracts registrales y evidencia distribuida previstas en esta ley operarán inicialmente como capas complementarias de integridad y prueba, sin sustituir las formalidades constitutivas, competencias notariales, calificación registral ni procedimientos establecidos por la legislación vigente.

Cuando una funcionalidad requiera modificar la forma constitutiva de un derecho real, acto notarial, asiento registral o procedimiento de inscripción, su implementación quedará condicionada a la reforma legal o reglamentaria específica que corresponda.

El Poder Ejecutivo, Registro Nacional, autoridades notariales e IID podrán desarrollar pilotos y propuestas de reforma dentro de sus competencias, con seguridad jurídica y protección de terceros.

Artículo 765. Coordinación Procesal y Probatoria

La evidencia on-chain, hashes, sellos de tiempo, firmas criptográficas, smart contracts y demás elementos técnicos reconocidos por esta ley serán admisibles conforme a las reglas procesales vigentes, sujetos a autenticidad, integridad, contradicción, pertinencia y valoración por la autoridad competente.

Ninguna disposición de esta ley modificará por sí sola la organización del Poder Judicial, la competencia de los tribunales ni reglas procesales cuya reforma requiera legislación especial. Las reformas que resulten necesarias se tramitarán mediante los procedimientos constitucionales correspondientes.

Artículo 766. Coordinación con la Legislación de Protección de Datos

Las obligaciones de identidad digital, biometría, credenciales verificables, trazabilidad, analítica on-chain e inteligencia artificial se interpretarán de manera compatible con la legislación de protección de datos personales y los derechos de autodeterminación informativa y privacidad.

Las técnicas de privacidad por diseño, minimización, pruebas de conocimiento cero, credenciales selectivas y almacenamiento descentralizado no reducirán los derechos del titular ni las obligaciones legales del responsable cuando exista tratamiento de datos personales.

La IID coordinará con la autoridad competente en protección de datos dentro de sus respectivos ámbitos, sin sustituir sus competencias.

Artículo 766 bis. Adición al Artículo 20 de la Ley N.° 7169

Adiciónase un inciso p) al artículo 20 de la Ley N.° 7169, Ley de Promoción del Desarrollo Científico y Tecnológico, para que se lea de la siguiente manera: “p) Ejercer la rectoría de la política pública nacional en materia de soberanía digital, tecnologías descentralizadas y emergentes, activos digitales e infraestructura tecnológica estratégica, en coordinación con las autoridades competentes y sin perjuicio de las competencias técnicas y regulatorias legalmente desconcentradas en la Intendencia de la Industria Descentralizada.”

Artículo 766 ter. Adición al Artículo 21 de la Ley N.° 7169

Adiciónase un párrafo final al artículo 21 de la Ley N.° 7169, Ley de Promoción del Desarrollo Científico y Tecnológico, para que se lea de la siguiente manera: “Las competencias que una ley especial atribuya a órganos de desconcentración máxima adscritos al Ministerio serán ejercidas exclusivamente por dichos órganos dentro del ámbito material expresamente desconcentrado. Respecto de esas competencias no procederán avocación, revisión o sustitución jerárquica, órdenes, instrucciones o circulares del jerarca ministerial, sin perjuicio de los controles de legalidad, presupuestarios, internos, externos y jurisdiccionales previstos por el ordenamiento.”

SECCIÓN IV — JERARQUÍA, INTERPRETACIÓN Y CONTROL DE CONSTITUCIONALIDAD

Artículo 767. Interpretación Pro Libertad Digital

Toda norma relacionada con activos digitales, blockchain, IA, identidad, autocustodia, criptografía, tokenización, DeFi, DAOs, datos, mercados digitales y tecnología deberá interpretarse conforme al principio pro libertad digital.

En caso de duda, deberá preferirse la interpretación que preserve derechos fundamentales, innovación lícita, autocustodia, privacidad, neutralidad tecnológica, propiedad digital y debido proceso.

Artículo 768. Principio de Máxima Protección de Derechos Digitales

Cuando existan varias interpretaciones posibles, deberá prevalecer aquella que brinde mayor protección a identidad digital soberana, privacidad, propiedad digital, libertad financiera, autocustodia, criptografía, no vigilancia masiva y dignidad humana.

Artículo 769. Control de Constitucionalidad Digital

Toda ley, reglamento, acto administrativo, contrato público, sistema tecnológico, algoritmo estatal, plataforma pública, mecanismo de identidad o infraestructura digital podrá ser sometido a control de constitucionalidad cuando pueda afectar derechos digitales fundamentales.

SECCIÓN V — CLÁUSULAS FINALES DE GARANTÍA Y ARMONIZACIÓN

Artículo 770. Cláusula Anti Autoritarismo Digital

Será contrario al orden constitucional todo sistema público o privado, cuando ejerza poder equivalente, que tenga por objeto o efecto:

a) Vigilancia masiva.
b) Scoring social.
c) Censura financiera.
d) Identidad digital obligatoria universal.
e) Control conductual automatizado.
f) CBDC obligatoria de vigilancia.
g) Perfilamiento político.
h) Biometría masiva indiscriminada.
i) Intermediación financiera obligatoria general.
j) Eliminación práctica de autocustodia.

Artículo 771. Cláusula de Soberanía Digital y Jerarquía Normativa

La aplicación interna de tratados, estándares, recomendaciones, compromisos internacionales, regulaciones extranjeras y políticas públicas en materias comprendidas por esta ley deberá realizarse de conformidad con la Constitución Política, la jerarquía normativa, los derechos fundamentales y los mecanismos de control de constitucionalidad aplicables.

Las recomendaciones, estándares técnicos y actos de cooperación que no tengan rango superior a la ley no podrán utilizarse para disminuir garantías establecidas por el ordenamiento interno. Los tratados internacionales vigentes conservarán la jerarquía y efectos que les reconoce la Constitución Política.

Artículo 772. Cláusula de Evolución Jurídica y Tecnológica

Los derechos y garantías digitales reconocidos en esta ley deberán interpretarse evolutivamente, conforme al avance de la tecnología, siempre en protección de la dignidad humana, libertad, privacidad, propiedad, democracia, seguridad jurídica y soberanía individual.

SECCIÓN VI — DERECHOS DIGITALES POST-MORTEM, SUCESIÓN CRIPTOGRÁFICA Y MEMORIA DIGITAL

Artículo 773. Reconocimiento de Derechos Digitales Post-Mortem

Toda persona tendrá derecho a disponer, ordenar, proteger, transferir, conservar, eliminar o limitar el uso de sus activos digitales, identidad digital, datos, credenciales, wallets, llaves, reputación digital, avatares, cuentas, contenidos, registros, IA personal, memoria digital y demás elementos patrimoniales o extrapatrimoniales de su vida

digital para después de su fallecimiento. Estos derechos deberán armonizarse con el derecho sucesorio, propiedad, privacidad, protección de datos, derechos de autor, derecho de imagen, secreto profesional y voluntad expresa de la persona fallecida.

Artículo 774. Testamento Criptográfico y Disposición Digital Sucesoria

Las personas podrán otorgar testamentos, instrucciones sucesorias, mandatos post-mortem, protocolos de recuperación o disposiciones digitales específicas sobre wallets, llaves privadas, cuentas, activos tokenizados, NFTs, credenciales, DAOs, datos, obras digitales, dominios, avatares, IA personal y demás bienes digitales. Dichas disposiciones podrán utilizar mecanismos criptográficos, multisig, custodios fiduciarios, notariado digital, smart contracts sucesorios, gestores de llaves, instrucciones cifradas o sistemas equivalentes, siempre que respeten formalidades legales aplicables, voluntad válida, seguridad y protección de terceros.

Artículo 775. Herencia de Activos Digitales y Llaves Criptográficas

Los activos digitales lícitamente poseídos por una persona formarán parte de su patrimonio sucesorio conforme a su naturaleza jurídica. La transmisión hereditaria de dichos activos deberá respetar autocustodia, seguridad de llaves, privacidad, existencia de beneficiarios designados, contratos inteligentes, reglas de protocolos, obligaciones tributarias aplicables y derechos de terceros. El Estado promoverá mecanismos seguros de recuperación y transmisión que no obliguen a revelar llaves privadas en vida ni a centralizar compulsivamente la custodia de activos.

Artículo 776. Identidad Digital, Cuentas y Reputación Post-Mortem

La identidad digital, cuentas, perfiles, credenciales, reputación, historial profesional, contenidos, archivos, publicaciones y presencia digital de una persona fallecida deberán administrarse conforme a su voluntad expresa, derechos de herederos, privacidad de terceros, términos compatibles con la ley y protección de dignidad post-mortem. Queda prohibida la explotación abusiva, suplantación, manipulación reputacional, monetización no autorizada o uso engañoso de la identidad digital de una persona fallecida.

Artículo 777. IA Personal, Avatares y Réplicas Digitales Post-Mortem

La creación, uso, entrenamiento, comercialización o difusión de avatares, voces sintéticas, imágenes, deepfakes, agentes conversacionales, gemelos digitales o sistemas de IA que simulen a una persona fallecida requerirá autorización expresa previa de la persona en vida o habilitación legal suficiente conforme a derechos de imagen, dignidad, privacidad, propiedad intelectual y derechos de herederos. Se prohíbe utilizar IA post-mortem para engañar, manipular, defraudar, explotar emocionalmente, alterar la memoria pública o crear representaciones incompatibles con la voluntad o dignidad de la persona fallecida.

Artículo 778. DAOs Familiares, Multisig Sucesorio y Gobernanza Patrimonial Digital

Las personas podrán estructurar mecanismos de gobernanza patrimonial digital mediante DAOs familiares, multisig, fideicomisos digitales, smart contracts sucesorios, designación de guardianes, custodios técnicos o reglas programables para administrar activos digitales, empresas tokenizadas, propiedad intelectual, derechos económicos, colecciones digitales y patrimonios descentralizados. Estos mecanismos deberán respetar orden público sucesorio, legítimas cuando correspondan, derechos de acreedores, protección de personas menores de edad, transparencia mínima y mecanismos de resolución de controversias.

Artículo 779. Derecho al Olvido, Conservación y Archivo Digital Post-Mortem

La persona podrá definir en vida si determinados datos, contenidos, cuentas, comunicaciones, imágenes, archivos, biometría, neurodatos, registros de actividad o memorias digitales deberán conservarse, transferirse, anonimizarse, eliminarse o restringirse después de su fallecimiento. La conservación de información de interés público, histórico, probatorio, contractual o patrimonial deberá equilibrarse con privacidad, dignidad, voluntad del titular y derechos de terceros.

Artículo 780. Armonización Civil, Notarial, Registral y Probatoria de la Sucesión Digital

El Poder Ejecutivo, la IID, el Registro Nacional, autoridades notariales, Poder Judicial y demás instituciones competentes deberán impulsar normas, protocolos y reformas para integrar activos digitales, testamentos criptográficos, evidencia on-chain, fe pública criptográfica, custodia de llaves, designación de beneficiarios digitales y prueba de titularidad digital en los procedimientos civiles, notariales, registrales, sucesorios y probatorios.

CAPÍTULO XXV — DISPOSICIONES TRANSITORIAS, IMPLEMENTACIÓN, MIGRACIÓN INSTITUCIONAL Y ENTRADA EN VIGENCIA

SECCIÓN I — ENTRADA EN VIGENCIA Y REGLAMENTACIÓN

Artículo 781. Vigencia Escalonada

La presente ley entrará en vigencia de forma escalonada conforme a los plazos expresamente establecidos en este capítulo y sus transitorios, a fin de garantizar seguridad jurídica, adaptación institucional, desarrollo técnico y protección de derechos.

Las disposiciones de derechos y garantías digitales, autocustodia, privacidad criptográfica, prohibición de vigilancia masiva y libertad financiera digital tendrán vigencia desde la publicación de la ley, salvo que una disposición concreta establezca un plazo distinto.

Las obligaciones esenciales, sanciones, tasas, licencias y restricciones sujetas a reserva de ley iniciarán en los plazos fijados por esta ley. El Poder Ejecutivo y la IID únicamente podrán calendarizar aspectos operativos, formularios, infraestructura, fases técnicas y migraciones dentro de los plazos máximos legalmente establecidos.

Artículo 782. Reglamentación Ejecutiva y Normativa Técnica

El Poder Ejecutivo emitirá los reglamentos ejecutivos necesarios para la aplicación de esta ley dentro de los plazos establecidos en las disposiciones transitorias. La IID y las demás autoridades competentes emitirán, dentro de sus respectivas habilitaciones legales, normas técnicas, disposiciones regulatorias de carácter general, criterios, guías y circulares para la ejecución de sus competencias.

La reglamentación y normativa técnica deberán respetar neutralidad tecnológica, proporcionalidad, consulta pública, autocustodia, privacidad, no vigilancia masiva, seguridad jurídica e innovación.

La normativa reglamentaria o técnica no podrá crear infracciones, sanciones, tributos, tasas, hechos generadores, nuevas categorías sustanciales de sujetos obligados, delitos, limitaciones de derechos fundamentales ni potestades de acceso a documentos privados no previstas expresamente por ley.

Artículo 783. Período General de Adaptación

Se establece un período general de adaptación de doce a veinticuatro meses para que sujetos regulados, entidades públicas, mercados, plataformas, VASP, bancos digitales, emisores, custodios, DAOs registradas, tokenizadores y demás actores profesionales ajusten sus operaciones a esta ley.

Durante dicho período, la IID deberá priorizar orientación, acompañamiento, sandbox, guías técnicas y planes de remediación antes que sanciones, salvo fraude, mala fe, riesgo grave, apropiación de fondos, lavado de dinero o daño a usuarios.

SECCIÓN II — IMPLEMENTACIÓN DE LA IID

Artículo 784. Instalación Inicial de la IID

La IID deberá quedar formalmente instalada dentro de los seis meses siguientes a la entrada en vigencia de esta ley, una vez cumplidos los procedimientos de organización, nombramiento, incorporación presupuestaria y control exigidos por el ordenamiento.

Durante la instalación, las autoridades preexistentes conservarán sus competencias vigentes. La transferencia de expedientes, registros o funciones solo ocurrirá mediante actos de transición expresamente definidos, garantizando continuidad, derechos adquiridos, debido proceso y ausencia de vacíos regulatorios.

Artículo 785. Programa Presupuestario Inicial y Recursos de Instalación

El Estado incorporará al Presupuesto Nacional los recursos iniciales necesarios para la instalación y operación de la IID. Durante sus primeros dos años podrán incorporarse progresivamente las tasas, derechos, registros y demás ingresos regulatorios autorizados por esta ley, todos sujetos al régimen presupuestario del Gobierno Central.

El uso de dichos recursos deberá estar sujeto a control interno, fiscalización de la Hacienda Pública, transparencia, rendición de cuentas y auditoría conforme al ordenamiento aplicable.

Artículo 786. Primeras Licencias, Registros y Sandbox

Durante el primer año de operación, la IID deberá habilitar:

a) Registro voluntario de VASP.
b) Registro de proyectos de tokenización.
c) Registro de DAOs.
d) Sandbox regulatorio nacional.
e) Consultas de clasificación de activos digitales.
f) Guías sobre Bitcoin, autocustodia y DeFi.
g) Guías sobre stablecoins y RWA.
h) Criterios iniciales de compliance criptográfico.

SECCIÓN III — MIGRACIÓN INSTITUCIONAL

Artículo 787. Adaptación del Sistema Bancario y Financiero

Las autoridades financieras deberán coordinar con la IID la adaptación gradual del sistema bancario y financiero para permitir interoperabilidad con activos digitales, VASP, bancos digitales, stablecoins, pagos blockchain, tokenización y autocustodia.

Durante la transición, quedará prohibido el debanking generalizado o automático de actores Web3 lícitos por el solo hecho de operar en la industria.

Artículo 788. Adaptación Registral

El Registro Nacional, Catastro, Registro de Personas Jurídicas, Registro de Garantías Mobiliarias, Registro de Propiedad Intelectual y demás registros deberán iniciar un plan gradual de interoperabilidad con infraestructura blockchain, fe pública criptográfica, sellos de tiempo, hashes y certificaciones verificables.

El plan deberá iniciar con pilotos de integridad documental y trazabilidad, sin afectar la validez del sistema registral vigente.

Artículo 789. Adaptación Judicial

El Poder Judicial, en el marco de su autonomía y de las decisiones que adopten sus órganos competentes, podrá desarrollar planes de capacitación y adecuación técnica para analizar y valorar evidencia on-chain, firmas criptográficas, smart contracts, DAOs, activos digitales, pruebas de conocimiento cero, identidad soberana y peritajes tecnológicos.

La IID y el MICITT podrán brindar cooperación técnica a solicitud de las autoridades judiciales, sin imponer organización, procedimientos internos, criterios jurisdiccionales ni obligaciones que invadan competencias constitucionalmente reservadas.

Artículo 790. Adaptación Tributaria

La Administración Tributaria deberá emitir guías interpretativas sobre territorialidad fiscal digital, Bitcoin, autocustodia, ganancias de capital, tokenización, DAOs, staking, minería, validadores, stablecoins y actividad empresarial Web3.

Dichas guías deberán respetar no tributación de mera tenencia, apreciación no realizada, transferencias entre wallets propias y autocustodia sin fuente costarricense.

Artículo 791. Adaptación Electoral

La autoridad electoral constitucionalmente competente podrá desarrollar, dentro de sus atribuciones exclusivas, una hoja de ruta de integridad electoral digital que contemple auditoría tecnológica, trazabilidad de procesos, sellos criptográficos, protección de identidad electoral, estándares abiertos y pilotos verificables cuando los considere compatibles con el ordenamiento electoral.

Ningún sistema de voto digital podrá implementarse al amparo exclusivo de esta ley ni sin las decisiones, pruebas, auditorías, garantías de secreto del voto, accesibilidad, ciberseguridad y controles que determine la autoridad electoral competente conforme a la Constitución Política y el Código Electoral.

SECCIÓN IV — IMPLEMENTACIÓN TECNOLÓGICA NACIONAL

Artículo 792. Estrategia Nacional Blockchain

El Poder Ejecutivo, en coordinación con la IID, deberá formular una Estrategia Nacional Blockchain dentro de los doce meses siguientes a la entrada en vigencia de esta ley.

La estrategia deberá incluir:

a) Gobierno digital.
b) Registro Público blockchain.
c) Anticorrupción.
d) Compras públicas.
e) Identidad soberana.
f) Tokenización.
g) Mercados digitales.

h) Educación.
i) Ciberseguridad.
j) Post-cuántica.
k) Interoperabilidad estatal.
l) Atracción de inversión.

Artículo 793. Interoperabilidad Pública

Las instituciones públicas deberán adoptar estándares de interoperabilidad, APIs seguras, identidad digital soberana, minimización de datos, trazabilidad, protección de datos y ciberseguridad para conectarse progresivamente con la infraestructura digital nacional.

Artículo 794. Inventario e implementación de infraestructura crítica digital

Dentro de los dieciocho meses siguientes a su instalación, la IID elaborará el primer inventario nacional de infraestructura digital crítica y emitirá un programa escalonado de auditorías técnicas de soberanía digital.

Las prioridades se definirán por impacto en derechos, continuidad de servicios esenciales, riesgo sistémico, exposición de datos, dependencia tecnológica, ciberseguridad y urgencia de migración criptográfica. Los órganos con competencias constitucionalmente exclusivas participarán mediante protocolos de coordinación que respeten su autonomía y reserva funcional.

Artículo 795. Pilotos Nacionales

La implementación de esta ley podrá iniciar mediante pilotos nacionales controlados, auditables y escalables en áreas como:

a) Registro Público blockchain.
b) Certificaciones verificables.
c) Compras públicas transparentes.
d) Tokenización de activos públicos no sensibles.
e) Identidad digital soberana voluntaria.
f) Sandbox financiero Web3.
g) Educación blockchain.
h) Arbitraje digital.
i) Trazabilidad presupuestaria.
j) Fe pública criptográfica.

SECCIÓN V — FORMACIÓN Y CAPACITACIÓN

Artículo 796. Capacitación Obligatoria Estatal

Las instituciones públicas vinculadas a la implementación de esta ley deberán capacitar progresivamente a sus funcionarios en derechos digitales, blockchain, activos digitales, ciberseguridad, privacidad, IA, evidencia digital, autocustodia, tokenización y protección de datos.

Artículo 797. Formación Técnica Nacional

El Estado promoverá programas de formación técnica con universidades, colegios profesionales, institutos, sector privado y comunidades Web3 para formar talento nacional en blockchain, IA, ciberseguridad, criptografía, smart contracts, ZKP, auditoría, post-cuántica y regulación digital.

SECCIÓN VI — TRANSICIÓN ECONÓMICA Y COMPETITIVA

Artículo 798. Atracción de Industria Web3

Durante los primeros tres años de vigencia, el Estado deberá impulsar un plan especial de atracción de empresas Web3, IA, blockchain, ciberseguridad, tokenización, infraestructura descentralizada, stablecoins, RWA, auditoría, arbitraje digital y compliance criptográfico.

Artículo 799. Transición Financiera Gradual

La coexistencia entre sistema financiero tradicional y sistema financiero descentralizado deberá implementarse gradualmente mediante:

a) Mesas técnicas.
b) Guías de interoperabilidad.
c) Protección contra debanking.
d) Pilotos de pagos blockchain.
e) Estándares AML/CFT proporcionales.
f) Educación bancaria.
g) Supervisión coordinada.
h) Pasarelas fiat-cripto reguladas.

Artículo 800. Competitividad Internacional

La IID deberá emitir un informe anual de competitividad internacional Web3, comparando a Costa Rica con otras jurisdicciones en materia de licencias, impuestos, incentivos, talento, infraestructura, derechos digitales, seguridad jurídica y atracción de inversión.

SECCIÓN VII — SUPERVISIÓN, EVALUACIÓN Y ACTUALIZACIÓN

Artículo 801. Evaluación Periódica del Modelo

La Asamblea Legislativa, la IID y las instituciones competentes deberán evaluar cada dos años la implementación de esta ley, su impacto económico, institucional, tecnológico, fiscal, social y constitucional.

La evaluación deberá incluir consulta pública con usuarios, industria, academia, comunidades técnicas, sector financiero, Poder Judicial, autoridades públicas y sociedad civil.

Artículo 802. Actualización Tecnológica Continua

La IID podrá proponer al Poder Ejecutivo y a la Asamblea Legislativa las reformas legales o reglamentarias que estime necesarias y, dentro de su competencia, emitir guías, criterios, normas técnicas y estándares para adaptar el marco regulatorio a nuevas tecnologías, amenazas, modelos de negocio, riesgos, estándares internacionales y avances científicos.

Toda actualización deberá respetar el núcleo de soberanía digital, autocustodia, privacidad, libertad financiera, debido proceso y prohibición de vigilancia masiva previsto en esta ley.

Artículo 803. Consejo Estratégico Nacional Web3

Créase el Consejo Estratégico Nacional Web3 como órgano consultivo de alto nivel, integrado por representantes de academia, sector privado, comunidades técnicas, IID, Poder Ejecutivo, sociedad civil y expertos independientes.

Su función será emitir recomendaciones sobre estrategia país, competitividad, educación, infraestructura, inversión, riesgos emergentes, estándares internacionales y evolución tecnológica.

Este Consejo no sustituirá a la IID ni tendrá potestades regulatorias vinculantes.

SECCIÓN VIII — CLÁUSULAS FINALES DE IMPLEMENTACIÓN

Artículo 804. Cláusula de Continuidad Estatal

La transición hacia infraestructura digital soberana deberá garantizar continuidad de servicios públicos, seguridad jurídica, protección de datos, estabilidad institucional y no afectación de derechos adquiridos.

Artículo 805. Cláusula de Resiliencia Democrática Digital

Toda implementación tecnológica derivada de esta ley deberá preservar democracia, privacidad, transparencia, derechos fundamentales, accesibilidad, auditabilidad, ciberseguridad y control ciudadano.

Artículo 806. Naturaleza de Ley Marco y Desarrollo Normativo Complementario

La presente ley tendrá naturaleza de Ley Marco en materia de soberanía digital, tecnologías emergentes, activos digitales, blockchain, inteligencia artificial, infraestructura financiera digital, identidad digital soberana, ciberseguridad, tokenización, democracia digital y derechos fundamentales digitales.

Su carácter marco permitirá el desarrollo progresivo de legislación especial, reglamentos técnicos, normas sectoriales, sandboxes, guías regulatorias y estándares institucionales complementarios, sin fragmentar la arquitectura sistémica de soberanía digital establecida en esta ley.

La legislación complementaria deberá respetar los principios de libertad digital, neutralidad tecnológica, interoperabilidad abierta, protección de derechos fundamentales, proporcionalidad, soberanía tecnológica, integridad financiera, prevención de vigilancia masiva y protección de innovación legítima.

Artículo 806 bis. Legislación complementaria especializada

La presente Ley Marco servirá como fundamento institucional, jurídico y técnico para el desarrollo posterior de leyes especializadas sobre activos digitales y VASP, inteligencia artificial, democracia tecnológica, neuroderechos, infraestructura digital soberana, transformación del Registro Público, notariado digital, zonas francas tecnológicas, infraestructura de mercado de activos digitales y demás materias vinculadas con la industria descentralizada.

La legislación complementaria deberá respetar los principios de soberanía digital democrática, neutralidad tecnológica, interoperabilidad internacional, proporcionalidad regulatoria, derechos fundamentales, seguridad jurídica, libre competencia, protección de privacidad y no vigilancia masiva.

La IID podrá elaborar propuestas técnicas, diagnósticos, consultas públicas, hojas de ruta, estudios de impacto y recomendaciones de política pública para apoyar el desarrollo progresivo de dicha legislación complementaria, sin sustituir la potestad legislativa de la Asamblea Legislativa ni las competencias constitucionales de otras instituciones.

Artículo 807. Modularidad Legislativa, Técnica e Institucional

La implementación de esta ley se realizará de forma modular, progresiva y coordinada, atendiendo a la naturaleza de cada bloque normativo, incluyendo derechos fundamentales digitales, activos digitales, infraestructura financiera, inteligencia artificial, ciberseguridad, identidad digital, tokenización, democracia digital, energía digital, régimen sancionatorio y cooperación internacional.

La modularidad no implicará separación conceptual ni pérdida de coherencia sistémica. Cada desarrollo reglamentario, institucional o legislativo deberá integrarse a la arquitectura general de soberanía digital de Costa

Rica.

El Poder Ejecutivo, la IID, las instituciones competentes y la Asamblea Legislativa podrán impulsar leyes complementarias o reformas especiales en materias de alta complejidad técnica, siempre que estas mantengan compatibilidad con la presente ley.

Artículo 808. Entrada en Vigencia Integral

La presente ley entrará en vigencia a partir de su publicación, sin perjuicio de los plazos escalonados de implementación técnica, reglamentaria e institucional aquí previstos.

Las autoridades competentes deberán adoptar las medidas necesarias para su ejecución gradual, coordinada y efectiva.

DISPOSICIONES TRANSITORIAS

Transitorio I. Instalación de la IID

La IID deberá instalarse dentro de los seis meses siguientes a la publicación de esta ley. El MICITT, en coordinación con el Ministerio de Planificación Nacional y Política Económica y el Ministerio de Hacienda en lo que corresponda, deberá realizar los ajustes organizativos, presupuestarios y administrativos necesarios para incorporar a la IID como órgano adscrito de desconcentración máxima, sin ubicarla jerárquicamente bajo un viceministerio o dirección sustantiva del Ministerio.

Dentro de los primeros noventa días posteriores a su instalación, el Consejo Técnico Superior deberá aprobar el reglamento interno de organización y funcionamiento, el código de ética, la política de conflictos de interés, el plan de supervisión inicial y el plan de transición regulatoria.

Transitorio II. Reglamentación Prioritaria

Dentro de los doce meses siguientes a la publicación de esta ley, deberán emitirse reglamentos prioritarios sobre:

a) VASP.
b) Clasificación de activos digitales.
c) Autocustodia y DeFi.
d) Stablecoins.
e) Tokenización RWA.
f) Sandbox regulatorio.
g) Compliance criptográfico.
h) Licencias y registros.
i) Protección al usuario.
j) Régimen sancionatorio.

Transitorio III. Sandbox Inicial

La IID deberá habilitar el Sandbox Regulatorio Nacional dentro de los nueve meses siguientes a su instalación.

Transitorio IV. Registro Provisional de Actores

Los VASP, tokenizadores, custodios, exchanges, plataformas de mercado, emisores y demás actores profesionales existentes podrán inscribirse provisionalmente durante los primeros doce meses posteriores a la habilitación del registro correspondiente.

La inscripción provisional permitirá operación transitoria bajo deberes mínimos de transparencia, AML/CFT proporcional, protección al usuario y buena fe regulatoria.

Transitorio V. No Sanción por Adaptación de Buena Fe

Durante el período de adaptación, no se impondrán sanciones por incumplimientos formales subsanables cuando el sujeto demuestre buena fe, cooperación, ausencia de daño, plan de remediación y voluntad de cumplimiento.

Esta disposición no aplicará a fraude, apropiación indebida, manipulación, lavado de dinero, captación ilícita, publicidad engañosa grave o daño a usuarios.

Transitorio VI. Hoja de Ruta del Registro Público Blockchain

El Registro Nacional deberá presentar dentro de los dieciocho meses siguientes a la publicación de esta ley una hoja de ruta para implementar:

a) Sellos criptográficos.
b) Hashes documentales.
c) Certificaciones verificables.
d) Interoperabilidad con Catastro.
e) Fe pública criptográfica.
f) Pilotos de tokenización registral.
g) Archivo histórico verificable.

Transitorio VII. Estrategia Nacional de Criptografía Post-Cuántica

El Poder Ejecutivo deberá presentar dentro de los veinticuatro meses siguientes una estrategia nacional de criptografía post-cuántica, criptoagilidad y protección de infraestructura crítica.

Transitorio VIII. Capacitación Judicial y Administrativa

El Poder Judicial, la IID y las instituciones competentes deberán iniciar programas de capacitación en evidencia digital, activos digitales, blockchain, IA, smart contracts, DAOs, ciberseguridad y derechos digitales dentro del primer año de vigencia.

Transitorio IX. Reforma y Armonización Normativa

El Poder Ejecutivo deberá presentar a la Asamblea Legislativa, dentro de los veinticuatro meses siguientes, un paquete de reformas complementarias para armonizar:

a) Código Civil.
b) Código de Comercio.
c) Ley de Mercado de Valores.
d) Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.
e) Ley de Certificados, Firmas Digitales y Documentos Electrónicos.
f) Normativa bancaria y financiera.
g) Normativa registral y notarial.
h) Normativa procesal y probatoria.
i) Normativa tributaria.
j) Normativa de contratación pública.

Transitorio X. Pilotos de Blockchain Anticorrupción

El Poder Ejecutivo deberá seleccionar al menos tres procesos públicos para pilotos de blockchain anticorrupción dentro de los primeros dieciocho meses, incluyendo preferentemente contratación pública, trazabilidad presupuestaria, certificaciones o registros administrativos.

Transitorio XI. Protección Inmediata de Autocustodia

Desde la publicación de esta ley, ninguna autoridad podrá prohibir, criminalizar, restringir o presumir ilícita la autocustodia legítima, salvo orden individualizada y motivada conforme a la Constitución y la ley.

Transitorio XII. Protección contra Debanking

Desde la publicación de esta ley, las entidades financieras no podrán aplicar políticas generales de exclusión contra personas o empresas por participar lícitamente en actividades Web3, blockchain, Bitcoin, activos digitales o autocustodia.

Transitorio XIII. Evaluación Inicial del Modelo

A los treinta y seis meses de entrada en vigencia, la Asamblea Legislativa deberá recibir un informe integral de evaluación sobre implementación, impacto, retos, riesgos, oportunidades y reformas necesarias.

Transitorio XIV. Adecuación Orgánica y Presupuestaria del MICITT

Dentro de los seis meses siguientes a la publicación de esta ley, el MICITT deberá someter y ejecutar las modificaciones de estructura organizacional necesarias para reflejar a la IID como órgano adscrito de desconcentración máxima. La estructura deberá asegurar separación funcional respecto de los viceministerios y direcciones sustantivas, apoyo administrativo compatible con la desconcentración y una identificación presupuestaria suficiente para el ejercicio de las competencias conferidas por esta ley.

La transición organizacional no podrá interrumpir servicios públicos, supervisión vigente, procedimientos administrativos ni obligaciones de cumplimiento. Los recursos humanos, tecnológicos y presupuestarios requeridos se incorporarán conforme al ordenamiento aplicable y a las autorizaciones presupuestarias correspondientes.