



Blockchain en la Gestión Pública
Hacia una Contabilidad Transparente y Descentralizada

Alumno: Maximiliano Obregón
Profesora de Trabajo Final: Marcela Samela

Trabajo Final de Carrera presentado para obtener el título de
Lic. en Gestión de Tecnología Informática

Julio, 2026

Resumen

En este trabajo se analizan desafíos de integridad, trazabilidad y disponibilidad de la información en los registros contables de la gestión pública, que dificultan la verificación oportuna y confiable y afectan la confianza ciudadana y la eficacia de la auditoría. Con el propósito de fortalecer la rendición de cuentas en organismos gubernamentales, se propone una solución basada en tecnología blockchain aplicada como mecanismo de registración y verificación de evidencia contable, en el marco de una propuesta de intervención en el campo profesional.

La propuesta contempla el diseño de una arquitectura blockchain híbrida que permita gestionar información sensible en un entorno permissionado y, en paralelo, anclar periódicamente resúmenes criptográficos (hashes) en una red pública. Este enfoque busca aportar garantías de integridad e inmutabilidad verificable sin comprometer la confidencialidad. La intervención se orienta a un piloto de aplicación en la Oficina Anticorrupción de la República Argentina, en función de su rol institucional en la promoción de la integridad y la prevención de la corrupción.

Asimismo, se define un esquema de implementación progresiva con instrumentos de medición y criterios de éxito, incluyendo mecanismos de privacidad por diseño y lineamientos para la verificación externa y social. Se espera que la propuesta contribuya a disminuir tiempos de verificación documental, reducir tareas manuales de conciliación y validación, minimizar inconsistencias en los registros y mejorar la trazabilidad de la evidencia contable, fortaleciendo así la capacidad de fiscalización y ofreciendo un modelo replicable para otros organismos del Estado.

Palabras clave: auditoría, blockchain, contabilidad gubernamental, sector público, transparencia

Abstract

In this work, challenges related to integrity, traceability, and availability of information in public sector accounting records are analyzed, as they hinder timely and reliable verification and affect public trust as well as audit effectiveness. In order to strengthen accountability within governmental bodies, a solution based on blockchain technology is proposed as a mechanism for the recording and verification of accounting evidence, within the framework of a professional field intervention proposal.

The proposal outlines a hybrid blockchain architecture that enables sensitive data management within a permissioned environment while periodically anchoring cryptographic summaries (hashes) to a public network. This approach aims to provide verifiable integrity and immutability guarantees without compromising confidentiality. The intervention is intended for a pilot implementation within the Oficina Anticorrupción of the Argentine Republic, given its institutional role in promoting integrity and preventing corruption.

Likewise, a phased implementation scheme is defined, including measurement instruments and success criteria, as well as privacy-by-design mechanisms and guidelines for external and social verification. The proposal is expected to contribute to reducing document verification times, decreasing manual reconciliation and validation tasks, minimizing inconsistencies in records, and improving the traceability of accounting evidence, thereby strengthening oversight capacity and providing a replicable model for other public sector entities.

Keywords: auditing, blockchain, government accounting, public sector, transparency

Índice general

Resumen	2
Abstract	3
Índice general.....	4
Índice de figuras.....	9
Índice de tablas	12
Capítulo 1: Introducción.....	15
1.1 Descripción del problema.....	15
1.2 Justificación de la propuesta.....	15
1.3 Marco institucional.....	16
1.4 Objetivos del trabajo final	16
1.4.1 <i>Objetivos generales</i>	16
1.4.2 <i>Objetivos particulares</i>	16
1.5 Resultados esperados.....	17
1.6 Contribuciones principales	17
Capítulo 2: Estado del arte	18
2.1 Panorama internacional y líneas de investigación	18
2.2 Aportes académicos en contabilidad y auditoría	22
2.2.1 <i>Introducción</i>	22
2.2.2 <i>Convergencias conceptuales: integridad, auditabilidad y “triple entrada”</i>	24
2.2.3 <i>Viabilidad económico-social vs. límites de adopción</i>	28
2.2.4 <i>Prospectiva en compras públicas</i>	31
2.2.5 <i>Evidencia y cadena de custodia</i>	32
2.2.6 <i>Competencias profesionales y aseguramiento sobre sistemas</i>	35
2.2.7 <i>Síntesis dialógica y vacíos de investigación</i>	37
2.3 Riesgos, barreras y marcos de control	40
2.4 Iniciativas y evidencias en América Latina	45
2.4.1 <i>Introducción</i>	45
2.4.2 <i>Perú - PERÚ COMPRAS en LACChain (contrataciones)</i>	47
2.4.3 <i>Colombia - bono digital en blockchain (regulación/finalidad)</i>	50
2.4.4 <i>Chile - CNE y notaría de datos (integridad/acceso)</i>	53
2.4.5 <i>Argentina - QuarkID y BFA (identidad/consorcio)</i>	54
2.4.6 <i>Síntesis y ruta de madurez</i>	57
2.5 Síntesis crítica y vacíos de investigación para Argentina	59

Capítulo 3: Marco teórico	62
3.1 Blockchain: concepto y fundamentos	62
3.2 Cómo funciona una red blockchain	66
3.3 Tipos de blockchain	69
3.3.1 Introducción	69
3.3.2 Redes públicas (permissionless)	70
3.3.3 Redes privadas	70
3.3.4 Redes permissionadas (de consorcio)	70
3.3.5 Arquitecturas híbridas	71
3.3.6 Criterios de elección	72
3.4 Beneficios para la gestión pública	74
3.5 Desafíos contables en el Estado	79
3.5.1 Introducción	79
3.5.2 Calidad, normalización e interoperabilidad de datos	81
3.5.3 Gobernanza, responsabilidades y control interno	85
3.5.4 Privacidad, confidencialidad y acceso a la información	89
3.5.5 Finalidad, rendimiento y continuidad operativa	95
3.5.6 Evidencia, auditoría y nuevos procedimientos	99
3.5.7 Integración con sistemas legados y continuidad documental	102
3.5.8 Custodia de claves y gestión de identidades	106
3.5.9 Costos, capacidades y gestión del cambio	109
3.5.10 Marco legal, validez probatoria y responsabilidad	112
3.5.11 Conclusiones	114
3.6 Marco normativo en Argentina	117
3.6.1 Introducción	117
3.6.2 Acceso a la información pública y transparencia activa	120
3.6.3 Protección de datos personales	121
3.6.4 Documentos electrónicos, firma digital y validez probatoria	123
3.6.5 Ética pública y prevención de la corrupción	123
3.6.6 Contrataciones públicas electrónicas y trazabilidad	124
3.6.7 Gobierno abierto y datos públicos reutilizables	126
3.6.8 Lineamientos públicos sobre blockchain y experiencias locales	127
3.6.9 Síntesis y brechas regulatorias	129
3.7 Aspectos éticos	132
3.7.1 Introducción	132
3.7.2 Principios rectores y deberes de integridad	133
3.7.3 Protección de datos personales y privacidad por diseño	134

3.7.4 Transparencia, trazabilidad y acceso a la información	138
3.7.5 Prevención de corrupción y soborno	138
3.7.6 Equidad, no discriminación e inclusión	139
3.7.7 Seguridad de la información y resiliencia	140
3.7.8 Gobernanza ética, rendición de cuentas y participación	142
3.7.9 Derechos de las personas y consentimiento	144
3.7.10 Ética de datos abiertos y publicación responsable	147
3.7.11 Sostenibilidad e impacto ambiental	149
Capítulo 4: Metodología	151
4.1 Enfoque metodológico	151
4.2 Alcances y limitaciones metodológicas	156
4.2.1 Introducción	156
4.2.2 Alcances	157
4.2.3 Limitaciones	160
4.2.4 Sesgos y validez	161
4.2.5 Fiabilidad	163
4.3 Proceso de validación técnica y teórica	165
4.4 Declaración de uso de inteligencia artificial	170
Capítulo 5: Desarrollo de la solución	170
5.1 Justificación del modelo híbrido	170
5.2 Diseño general del sistema	173
5.3 Módulos funcionales	179
5.4 Protección de la información	182
5.5 Contratos inteligentes y validación	185
5.6 Participación ciudadana e incentivos	187
5.7 Casos de uso y simulaciones	189
5.8 Diagramas técnicos	192
Capítulo 6: Plan de implementación	193
6.1 Elección del organismo público	194
6.1.1 La Oficina Anticorrupción: historia y creación	194
6.1.2 Cómo funcionan hoy sus procesos (síntesis operativa)	194
6.1.3 Criterios de selección de la OA	195
6.1.4 Implementación en los procesos actuales	196
6.2 Etapas del despliegue	197
6.3 Recursos humanos necesarios	203

6.3.1 Estructura del equipo (núcleo del piloto)	204
6.3.2 Responsabilidades y entregables por rol	205
6.3.3 Matriz RACI (detallada)	206
6.3.4 Plan de dotación por fases (FTE y momentos de mayor carga)	209
6.3.5 Capacidades y plan de fortalecimiento	210
6.3.6 Indicadores de desempeño del equipo (KPIs)	210
6.4 Diagrama de Gantt de implementación	210
6.5 Infraestructura tecnológica y costos	213
6.5.1 Arquitectura de referencia	213
6.5.2 Decisiones de diseño y supuestos	214
6.5.3 Dimensionamiento y rendimiento esperado (piloto 12 meses)	215
6.5.4 Estimación referencial de costos (capex/opex)	216
6.5.5 Riesgos técnicos y mitigaciones	218
6.6 Aspectos legales y regulatorios	219
6.6 Indicadores e instrumentos de medición	220
6.6.1 Definiciones operacionales y metas	220
6.6.2 Instrumentos y método de medición	224
6.6.3 Gobierno de la medición y aseguramiento	225
6.6.4 Criterios de éxito	226
6.7 Gestión del cambio y capacitación	227
6.7.1 Objetivos y principios	228
6.7.2 Comunicación y acompañamiento operativo	228
6.7.3 Formación por perfil (currícula, evaluación y certificación)	228
6.7.4 Prácticas y simulacros	229
6.7.5 Cronograma, responsabilidades, métricas y refuerzo	230
6.8 Riesgos y mitigación	233
6.8.1 Taxonomía y apetito de riesgo	233
6.8.2 Registro de riesgos y mitigación (resumen operativo)	234
6.8.3 Señales tempranas (EWI) y umbrales de escalamiento (RAG)	239
6.8.4 Plan de anclaje híbrido (operación y contingencias)	240
6.8.5 Gobernanza del riesgo y verificación independiente	241
6.9 Resumen	242
Capítulo 7: Evaluación e impacto.....	243
7.1 Comparación con modelos tradicionales	243
7.2 Beneficios esperados	246
7.3 Limitaciones del enfoque propuesto	250
7.4 Escalabilidad y replicabilidad	253

7.5 Alineación con estrategias globales	256
7.6 Conclusiones preliminares	259
Capítulo 9: Factores condicionantes	261
9.1 Condicionantes institucionales, normativos y operativos.....	261
9.2 Viabilidad institucional, sostenibilidad y dependencia tecnológica	263
Conclusiones.....	264
Trabajos futuros.....	267
Anexos.....	269
Anexo 1: Criterios de Admisibilidad Probatoria de Evidencia Blockchain.....	269
Anexo 2: Playbooks de Respuesta a Incidentes en la Red Blockchain	273
Anexo 3: Modelo Energético y Huella Operativa de la Solución.....	277
Anexo 4: Carta de Gobernanza de la Red Blockchain y Reglas del Consorcio	279
Acrónimos	282
Referencias	283

Índice de figuras

Figura 1 Panorama internacional de adopción	18
Figura 2 Caso Estonia: patrón de diseño.....	20
Figura 3 Triángulo de valor en contabilidad pública	25
Figura 4 Doble entrada vs. triple entrada.....	26
Figura 5 Curva beneficio público vs. madurez de adopción.....	29
Figura 6 Cadena de evidencia en compras con publicación responsable.....	32
Figura 7 Mapa de competencias para auditoría en entornos blockchain	36
Figura 8 Mapa de convergencias y tensiones 2020–2025.....	39
Figura 9 Mapa de calor de riesgos	42
Figura 10 Flujo de evidencia aceptable según ISSAI 100	44
Figura 11 Mapa regional de iniciativas por dominio	46
Figura 12 Flujo técnico de publicación de órdenes de compra en PERÚ COMPRAS.....	48
Figura 13 Cadena de custodia verificable.....	50
Figura 14 Arquitectura del piloto: emisora y tenedor en LACChain.....	51
Figura 15 Línea de tiempo del bono digital	52
Figura 16 Pipeline de certificación CNE	53
Figura 17 Modelo de acceso e integridad	54
Figura 18 Arquitectura QuarkID.....	55
Figura 19 Ruta de madurez y escalamiento	58
Figura 20 Esquema conceptual de blockchain.....	63
Figura 21 Capas de una plataforma con contratos inteligentes.....	64
Figura 22 Mapa conceptual de tipos	69
Figura 23 Esquema de anclaje híbrido.....	72
Figura 24 Modelo propuesto para la OA	74
Figura 25 Mapa de beneficios por dimensión.....	76
Figura 26 Teoría de cambio del proyecto.....	77
Figura 27 Taxonomía de desafíos blockchain en contabilidad pública.....	80
Figura 28 Pipeline de calidad e interoperabilidad (antes del on-chain).....	83
Figura 29 Diagrama de flujo de gobernanza del consorcio	86
Figura 30 Flujo de publicación con privacidad.....	91
Figura 31 Modelo de capas de acceso.....	95
Figura 32 Curvas conceptuales rendimiento–latencia	97
Figura 33 Arquitectura de continuidad operativa en red permissionada	98

Figura 34 Cadena de custodia digital.....	100
Figura 35 Mapa de competencias para auditoría blockchain.....	102
Figura 36 Arquitectura de integración y cadena de custodia	103
Figura 37 Secuencia de integración idempotente	105
Figura 38 Gobernanza de claves e identidades	107
Figura 39 Flujo de autorización con MFA y co-firma por umbral.....	108
Figura 40 Mapa radial de capacidades y brechas.....	110
Figura 41 Curva de madurez y gestión del cambio.....	111
Figura 42 Ciclo de vida probatorio de un documento digital	113
Figura 43 Ruta de decisión para adoptar blockchain contable en el Estado	115
Figura 44 Resumen visual de beneficios vs. riesgos.....	117
Figura 45 Línea de tiempo de hitos regulatorios (2001–2025).....	120
Figura 46 Mapa de actores y lineamientos públicos sobre blockchain.....	128
Figura 47 Marco de principios éticos ↔ controles y métricas	133
Figura 48 Seguridad de la información y resiliencia: ciclo evidencia-control-verificación	141
Figura 49 Gobernanza ética y rendición de cuentas (RACI)	143
Figura 50 Flujo de datos on/off-chain con consentimiento y derechos ARCO (swimlanes)	146
Figura 51 Mapa del diseño mixto (visión ejecutiva).....	152
Figura 52 Flujo metodológico end-to-end (BPMN simple).....	156
Figura 53 Cadena de custodia y trazabilidad de datos (swimlanes)	158
Figura 54 RACI metodológico (swimlanes)	159
Figura 55 Mapa de riesgos de validez y fiabilidad (heatmap)	163
Figura 56 Trazabilidad on/off-chain del piloto metodológico (grafo)	166
Figura 57 Diagrama de contexto (alcance y actores).....	173
Figura 58 Arquitectura lógica de red híbrida	174
Figura 59 Despliegue y seguridad (nodos, zonas, HSM/KMS).....	179
Figura 60 Componentes y módulos (visión C4-Container)	182
Figura 61 Modelo de datos y metadatos mínimos (ER).....	183
Figura 62 Secuencia del registro contable con smart contracts (UML).....	186
Figura 63 Roadmap del despliegue (E0–E6) con gates y entregables	199
Figura 64 Organigrama funcional.....	205
Figura 65 Cronograma de implementación del piloto	212
Figura 66 Balance de costos: CAPEX/OPEX y fees de anclaje (escenario piloto).	217
Figura 67 Arquitectura de medición y aseguramiento de KPIs	225

Figura 68 Latencia documento→anclaje y cobertura con hash (metas vs. línea base).....	227
Figura 69 Cronograma de adopción y capacitación (12 semanas) con métricas de avance.....	230
Figura 70 Mapa de riesgos del piloto (heatmap probabilidad×impacto)	234
Figura 71 Política de anclaje híbrido multired (operación y contingencias)	241
Figura 72 Flujo de evidencia: modelo tradicional vs. blockchain	244
Figura 73 Teoría del cambio de la intervención.....	247
Figura 74 Arquitectura de privacidad on/off-chain.....	251
Figura 75 Hoja de ruta de expansión (0–18+ meses).....	255

Índice de tablas

Tabla 1 Síntesis de guías internacionales y focos recomendados.....	19
Tabla 2 Líneas de investigación y brechas de conocimiento.....	21
Tabla 3 Matriz comparativa de tesis y artículos	23
Tabla 4 Artefactos de evidencia y procedimientos de auditoría	27
Tabla 5 Condiciones habilitantes para triple entrada útil	28
Tabla 6 Matriz de decisión de adopción.....	30
Tabla 7 Matriz on-chain/off-chain para evidencia contable	34
Tabla 8 Matriz de competencias vs. actividades de aseguramiento	37
Tabla 9 Agenda de investigación.....	40
Tabla 10 Matriz riesgo-control (enfoque COSO)	43
Tabla 11 Checklist de gobernanza (redes permissionadas).....	45
Tabla 12 Inventario regional de pilotos y métricas	47
Tabla 13 Parámetros de implementación PERÚ COMPRAS	49
Tabla 14 Comparación QuarkID-BFA.....	56
Tabla 15 Comparación entre base de datos centralizada y blockchain en uso público	65
Tabla 16 Comparativa de mecanismos de consenso para redes públicas y permissionadas	67
Tabla 17 Comparativa por dimensiones	71
Tabla 18 Matriz de decisión	73
Tabla 19 Beneficios por proceso y organismo	77
Tabla 20 Indicadores propuestos de beneficio	78
Tabla 21 Síntesis de riesgos y líneas de mitigación	81
Tabla 22 Pipeline de calidad e interoperabilidad (resumen operativo)	85
Tabla 23 RACI de gobernanza (roles por actividad).....	87
Tabla 24 Umbrales de votación para acciones sensibles	89
Tabla 25 Matriz on-chain/off-chain y base legal.....	92
Tabla 26 Comparativa de técnicas de privacidad aplicables	94
Tabla 27 Plexo normativo y efectos para blockchain en la gestión pública (Argentina)	119
Tabla 28 Contrataciones electrónicas: principios ↔ controles ↔ evidencias on/off-chain.....	126
Tabla 29 Síntesis de brechas regulatorias y mitigaciones	131
Tabla 30 Matriz ética de riesgo-control-evidencia (privacy-by-design)	135
Tabla 31 Checklist EIPD para proyectos con blockchain	137
Tabla 32 Ética de datos abiertos: criterios de publicación responsable.....	148
Tabla 33 Mapa del diseño mixto (conexión y fusión)	153

Tabla 34 Operacionalización de indicadores.....	154
Tabla 35 Plan de análisis	155
Tabla 36 Calendario y hitos del trabajo de campo	157
Tabla 37 RACI metodológico	160
Tabla 38 Riesgos de validez y salvaguardas	162
Tabla 39 Protocolo de recolección y cadena de custodia	164
Tabla 40 Scripts y reproducibilidad	165
Tabla 41 Muestreo y estratificación para verificación	167
Tabla 42 Trazabilidad on/off-chain del piloto metodológico	167
Tabla 43 Criterios de aceptación por métrica	168
Tabla 44 Matriz procedimiento–control (enfoque auditoría)	168
Tabla 45 Matriz on/off chain y base legal	171
Tabla 46 Plan de anclaje híbrido (permisionada ↔ pública)	172
Tabla 47 Metadatos críticos y justificación de minimización	175
Tabla 48 Matriz RACI de gobernanza multi-actor.....	176
Tabla 49 Controles por capa vs. ISO/IEC 27001–27701 y legislación aplicable.....	177
Tabla 50 SLO/SLA y umbrales de desempeño.....	178
Tabla 51 Eventos de contrato inteligente y esquema de registro (log).....	181
Tabla 52 Riesgos y salvaguardas EIPD por módulo	184
Tabla 53 Datasets de transparencia activa y sensibilidad.....	188
Tabla 54 Métricas de participación y control social.....	189
Tabla 55 Simulaciones: parámetros y criterios de aceptación.....	190
Tabla 56 Catálogo de verificaciones reproducibles.....	191
Tabla 57 Etapas del despliegue, objetivos, gates y entregables (E0–E6).....	198
Tabla 58 Matriz RACI detallada por actividad	208
Tabla 59 Plan de dotación por fases (FTE y picos de carga).....	209
Tabla 60 Supuestos de dimensionamiento y rendimiento del piloto (12 meses).....	215
Tabla 61 Estimación referencial de costos (CAPEX/OPEX) por rubro	216
Tabla 62 Definiciones operacionales de indicadores (T1–T12), metas y gobierno.....	223
Tabla 63 Cronograma de capacitación por rol y métricas de adopción (Capacitación)	232
Tabla 64 Cronograma de capacitación por rol y métricas de adopción (Semanas).....	233
Tabla 65 Registro de riesgos del piloto, mitigaciones y EWI/RAG.....	238
Tabla 66 Política de anclaje multired y contingencias	240
Tabla 67 Comparación sintética entre modelos tradicionales y la propuesta basada en blockchain.....	245

Tabla 68 Beneficios esperados e indicadores clave de desempeño (KPI).....	249
Tabla 69 Palancas de escalabilidad y criterios de replicabilidad.....	254
Tabla 70 Mapa de alineación entre la intervención y estrategias globales.....	258

Capítulo 1: Introducción

1.1 Descripción del problema

En el sector público argentino, los registros contables y presupuestarios constituyen un insumo crítico para la rendición de cuentas, el control interno y la auditoría externa. Sin embargo, en la práctica persisten desafíos vinculados con la integridad, la trazabilidad y la disponibilidad de la información a lo largo del ciclo de gestión del gasto, lo que puede dificultar verificaciones oportunas y consistentes y, en consecuencia, debilitar mecanismos de fiscalización y control social. Estos desafíos se observan en contextos donde la transformación digital avanza de forma heterogénea y donde los datos públicos requieren criterios de calidad, interoperabilidad y publicación responsable para ser reutilizables y auditables (Banco Mundial, 2022; Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2020; World Wide Web Consortium [W3C], 2017; International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2008).

En Argentina, la administración financiera y los sistemas de control del sector público se enmarcan en normas específicas que definen responsabilidades, procesos y principios para la registración y el control (Ley 24.156, 1992). En este marco, existen sistemas transaccionales y plataformas de registración que apoyan la gestión financiera; no obstante, en escenarios reales pueden emerger limitaciones operativas y de arquitectura de información relacionadas con integración entre sistemas, trazabilidad extremo a extremo y mecanismos de verificación independientes, aspectos relevantes para auditorías del sector público basadas en evidencia suficiente y apropiada (International Organization of Supreme Audit Institutions [INTOSAI], 2013; Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013).

1.2 Justificación de la propuesta

Esta propuesta se fundamenta en una necesidad concreta: fortalecer la confiabilidad y la auditabilidad de los registros contables públicos mediante un enfoque que incremente garantías de integridad y trazabilidad, con criterios verificables por distintos actores. Desde la perspectiva de la integridad pública, mejorar la disponibilidad y la verificabilidad de la información contribuye a robustecer la rendición de cuentas y las capacidades de control, en línea con recomendaciones internacionales de integridad y gobierno digital (OCDE, 2017, 2020).

Desde una perspectiva técnica, se explora un diseño basado en tecnología blockchain como capa de registración y verificación que permita incorporar propiedades de inmutabilidad verificable y trazabilidad criptográfica, integrándose con procesos existentes sin sustituir de forma inmediata los sistemas vigentes. Este enfoque busca complementar el control interno y facilitar prácticas de auditoría orientadas a

evidencia, alineadas con principios de auditoría del sector público (INTOSAI, 2013) y con marcos de control interno ampliamente utilizados (COSO, 2013).

En este marco, corresponde precisar que la propuesta no implica sustituir los principios contables vigentes en la República Argentina ni alterar el plexo normativo que rige la registración, el control y la rendición de cuentas en el sector público. Su alcance es complementario y tecnológico: incorporar una capa adicional de evidencia digital verificable, trazabilidad criptográfica y validación técnica sobre registros y documentos producidos conforme a los procedimientos actualmente exigibles. Bajo esta lógica, la tecnología blockchain no se plantea como reemplazo del régimen contable aplicable, sino como un instrumento orientado a fortalecer la confiabilidad, la auditabilidad y la integridad de la información.

Desde una mirada metodológica-aplicada, el trabajo propone un prototipo funcional y un esquema de evaluación con criterios explícitos (indicadores e instrumentos de medición), lo que permite una validación más transparente y replicable del aporte, evitando formulaciones meramente declarativas.

1.3 Marco institucional

La intervención se orienta a la Oficina Anticorrupción (OA) de la República Argentina, creada en el ámbito del Poder Ejecutivo Nacional y con funciones vinculadas a la prevención de la corrupción, la promoción de la integridad y el fortalecimiento de mecanismos institucionales de transparencia (Decreto 102/1999, 1999; Oficina Anticorrupción [OA], s. f.). La elección del organismo se justifica por su rol transversal y su vinculación con políticas de integridad pública.

En términos de alcance, la propuesta considera un piloto aplicable al registro y seguimiento de operaciones internas asociadas a la ejecución del gasto y contrataciones, incorporando una capa adicional de trazabilidad e integridad verificable sobre eventos relevantes del proceso. La disponibilidad de evidencia con mayor trazabilidad es consistente con prácticas de control y auditoría que requieren documentación verificable y criterios claros de revisión (COSO, 2013; INTOSAI, 2013).

1.4 Objetivos del trabajo final

1.4.1 Objetivos generales

Diseñar una arquitectura de referencia para un sistema de registración contable pública basado en tecnología blockchain y especificar su esquema de evaluación, orientado a fortalecer la integridad, la trazabilidad y la verificabilidad de los registros financieros, con criterios de auditoría y medición explícitos.

1.4.2 Objetivos particulares

- a) Definir una arquitectura blockchain híbrida que equilibre confidencialidad de datos institucionales con verificabilidad externa mediante anclajes criptográficos.

- b) Especificar módulos funcionales orientados a registraci3n contable, auditoría y publicaci3n de informaci3n bajo criterios de transparencia y trazabilidad.
- c) Especificar contratos inteligentes (eventos, validaciones y reglas de negocio) orientados a automatizar controles relevantes en el ciclo del gasto.
- d) Establecer criterios e indicadores medibles para evaluar el desempeo e impacto institucional del prototipo.
- e) Proponer mecanismos viables de verificaci3n externa y participaci3n ciudadana, considerando incentivos no monetarios y restricciones tcnicas y contextuales.

El alcance de este trabajo se concentra en la arquitectura de referencia, la especificaci3n funcional y el esquema de evaluaci3n. La implementaci3n, despliegue validaci3n empírica de los indicadores propuestos quedan planteados como piloto.

1.5 Resultados esperados

Se espera que la propuesta: (i) reduzca fricciones operativas de auditoría y verificaci3n al automatizar y estandarizar la generaci3n de evidencias; (ii) fortalezca la confianza en la informaci3n contable al incorporar trazabilidad y verificabilidad distribuida de los registros; (iii) mejore la oportunidad y la trazabilidad de la ejecuci3n presupuestaria sin exponer datos sensibles; y (iv) ofrezca un modelo replicable para otros organismos del sector pblico, alineado con lineamientos de integridad y gobierno digital (OCDE, 2017, 2020; Banco Mundial, 2022).

1.6 Contribuciones principales

La contribuci3n central del trabajo es un diseo tcnico aplicable al contexto pblico argentino que agrega garantías criptogrficas de integridad y trazabilidad a la evidencia contable, complementando los controles y prcticas de auditoría vigentes. En concreto, se propone: (i) un enfoque de registraci3n verificable e inmutable para eventos contables relevantes; (ii) lineamientos de integraci3n con procesos y sistemas existentes, evitando soluciones aisladas; y (iii) un esquema de evaluaci3n con indicadores e instrumentos de medici3n orientados a auditoría basada en evidencia (COSO, 2013; INTOSAI, 2013).

Estas contribuciones buscan traducir el consenso internacional sobre blockchain y contabilidad pblica en un diseo operativo y medible para la Oficina Anticorrupci3n y, potencialmente, para otras entidades del sector pblico.

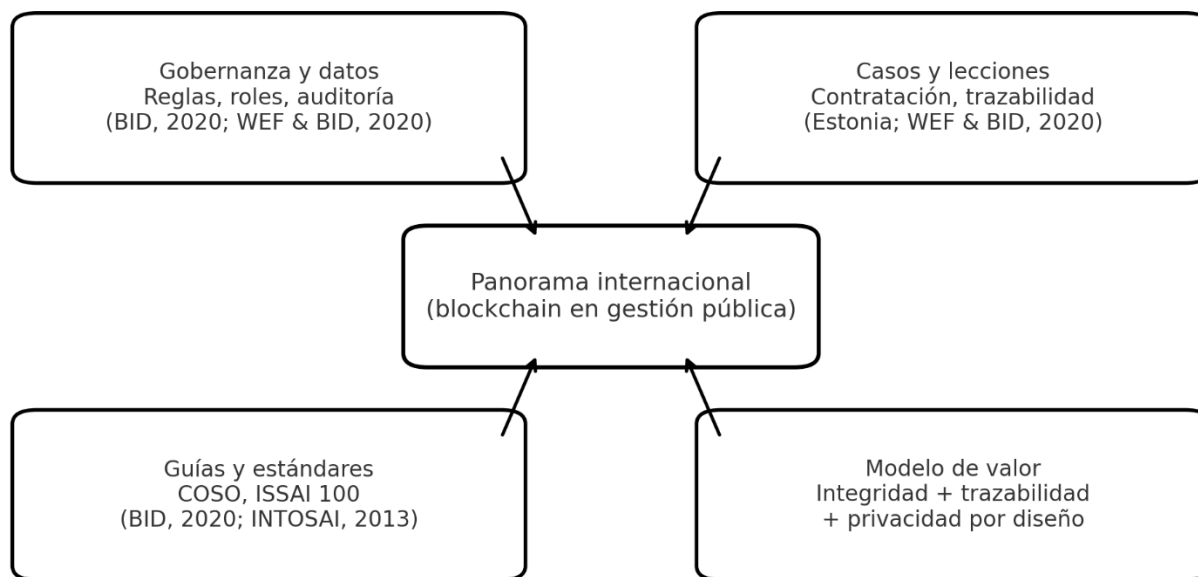
Capítulo 2: Estado del arte

2.1 Panorama internacional y líneas de investigación

A escala global, la literatura converge en que *blockchain* aporta integridad, trazabilidad y auditabilidad a los registros públicos cuando su adopción se inserta en marcos de gobernanza y de datos bien definidos. El Banco Interamericano de Desarrollo presenta la tecnología como infraestructura habilitante para gobiernos abiertos, subrayando la utilidad de *sellos de tiempo*, firmas y evidencias criptográficas replicadas en múltiples nodos para sostener la confianza en procesos críticos (Banco Interamericano de Desarrollo [BID], 2020). De modo complementario, el Foro Económico Mundial y el BID documentan aplicaciones en contratación pública (trazabilidad de expedientes y de hitos contractuales) y enfatizan que el valor público emerge cuando la solución técnica se alinea con reglas claras de datos, roles y auditoría interinstitucional, más que por la tecnología per se (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). En este contexto, la Figura 1 sintetiza el panorama internacional de adopción de blockchain en el sector público, diferenciando dominios de uso y nivel de madurez.

Figura 1

Panorama internacional de adopción



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); e-Estonia (2021).

En cuanto a experiencias internacionales, Estonia se convirtió en un referente de *integridad verificable* para registros estatales (salud, justicia, catastro), apoyándose en infraestructuras criptográficas y anclajes para garantizar la no alteración sin exponer contenido sensible (e-Estonia, 2021). Este patrón — inmutabilidad verificable, privacidad por diseño y gobernanza explícita— se replica en distintos proyectos públicos y condensa una lección central del estado del arte: *blockchain* funciona mejor como componente dentro de arquitecturas de gobierno digital y de control, no como un fin autosuficiente (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 1 resume las principales guías y marcos internacionales relevantes para blockchain en gestión pública, destacando sus focos y aportes metodológicos.

Tabla 1
Síntesis de guías internacionales y focos recomendados

Fuente	Alcance	Recomendaciones clave	Implicancias contabilidad pública
BID (2020)	Gobierno abierto + blockchain en ALC	Definir consorcio y gobierno de datos; elegir caso con metas medibles.	Contabilidad programable; trazabilidad con anclaje público.
Foro Económico Mundial & Banco Interamericano de Desarrollo (2020)	Compras públicas en blockchain	Roles/membresía claros; hitos verificables; privacidad por diseño; monitoreo.	Expedientes y pagos trazables; menos discrecionalidad; evidencia auditable.
INTOSAI (2013) – ISSAI 100	Principios de auditoría pública	Evidencia suficiente; criterios claros; papeles de trabajo trazables.	Mapear hashes/logs a pruebas sustantivas y de cumplimiento.
COSO (2013/2020)	Control interno y gestión de riesgos	Ambiente, riesgos, controles, info/comunicación y monitoreo.	Segregación en validación/despliegue; matrices de riesgo; monitoreo de contratos/nodos.

Nota. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); International Organization of Supreme Audit Institutions (2013); Committee of Sponsoring Organizations of the Treadway Commission (2013, 2020).

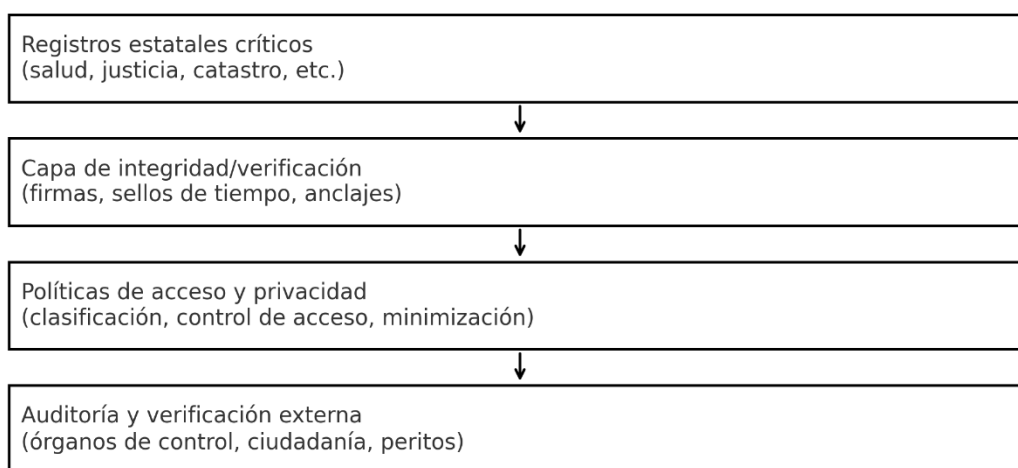
Morales (2021) destaca que la irrupción de blockchain abre la posibilidad de reorganizar el intercambio de datos contables reduciendo intermediarios, y apoyándose en registros distribuidos que todos los participantes pueden verificar, lo que refuerza la confiabilidad y dificulta la alteración posterior de la

información (p. 348). En esta línea, la discusión académica reciente se desplaza desde la idea de “subir todo a la cadena” hacia el diseño de sistemas de registro que disminuyan conciliaciones manuales, habiliten esquemas de auditoría continua y generen trazas completas para el control.

Asimismo, Morales (2021) plantea que blockchain puede introducir mejoras relevantes en los sistemas de información contable y en la calidad de los datos, justamente porque se basa en una base de datos distribuida resistente a la manipulación; sin embargo, esto obliga a replantear los enfoques clásicos de evaluación de riesgos y de diseño de controles, en lugar de eliminarlos (p. 348). La Figura 2 ilustra el patrón de diseño aplicado en Estonia para asegurar integridad verificable de registros estatales mediante anclajes criptográficos y segregación de datos sensibles.

Figura 2

Caso Estonia: patrón de diseño



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en e-Estonia (2021).

A su vez, la literatura advierte sobre el grado de madurez. Santos, tras revisar aportes técnicos (contratos inteligentes, contabilidad de triple entrada) y normativos, concluye que la adopción “no está aún generalizada”, aunque el potencial transversal es alto si se cierran brechas de competencias y se enmarcan los desarrollos en estándares y regulación adecuados (Santos, 2022).

De este modo, las líneas de investigación más citadas se ordenan en tres frentes. Primero, aplicaciones sustantivas en gasto y compras públicas (*procure-to-pay*, hitos de obra), identidad y certificaciones, y contabilidad gubernamental con controles ex ante programables mediante contratos inteligentes (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Santos, 2022). Segundo, gobernanza y control interno, donde los marcos COSO recomiendan políticas de

membresía, segregación de funciones, *change management* y monitoreo continuo para que la “inmutabilidad” técnica se traduzca en responsabilidades trazables (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013, 2020). Tercero, auditoría y evidencia, con ISSAI 100 como referencia para definir qué es “evidencia suficiente y apropiada” en entornos con *hashes*, *logs* de eventos y pruebas criptográficas, y cómo se custodia esa evidencia sin vulnerar restricciones legales (International Organization of Supreme Audit Institutions [INTOSAI], 2013).

El estado del arte internacional muestra convergencia conceptual y pilotos sectoriales que avanzan desde la demostración técnica hacia el encaje institucional: calidad e interoperabilidad de datos, privacidad por diseño, gobernanza interinstitucional y validación regulatoria de la evidencia. Para América Latina, los informes Foro Económico Mundial & Banco Interamericano de Desarrollo recomiendan redes permissionadas con anclaje público y modelos de datos bien gobernados, mientras que la literatura en contabilidad y auditoría (Morales, 2021; Santos, 2022) interpela a la profesión y a los organismos de control a desarrollar nuevas capacidades. Este trabajo se inscribe en ese punto de madurez: toma como base el consenso internacional y orienta la contribución hacia un prototipo aplicado en contabilidad pública con métricas de desempeño y control, enlazando el componente tecnológico con las reglas de juego que le dan sentido. La Tabla 2 organiza las principales líneas de investigación detectadas en la literatura reciente y las brechas de conocimiento pendientes en contabilidad pública y blockchain.

Tabla 2
Líneas de investigación y brechas de conocimiento

Línea/tema	Hallazgos consistentes	Desafíos abiertos	Oportunidades
Contratación pública (blockchain)	Trazabilidad de expedientes y pagos; menor discrecionalidad.	Integración con plataformas; privacidad de ofertas; gobernanza.	Hitos con anclaje público y panel de auditoría.
Controles ex ante (smart contracts)	Automatiza reglas y autorizaciones; registros inmutables.	Lógica correcta; excepciones/reversiones; desempeño.	Segregación de funciones y bitácora de cambios.
Gobernanza y control interno (COSO/ISSAI)	Responsabilidades trazables; evidencia suficiente.	Membresía, custodia de claves y cambios.	Matriz de roles/quóruns; auditorías periódicas.
Privacidad por diseño / anclaje público	Integridad verificable sin exponer datos.	Partición on/off-chain; reidentificación; base legal.	Esquema híbrido (hashes/sellos); vistas por audiencia.

Auditoría continua y analítica on-chain	Monitoreo casi en tiempo real con alertas.	Capacidades; estandarizar eventos/logs.	Catálogo de eventos; tablero de riesgos; capacitación.
---	--	---	--

Nota. Elaboración propia a partir de Morales (2021); Santos (2022); Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); International Organization of Supreme Audit Institutions (2013); Committee of Sponsoring Organizations of the Treadway Commission (2013, 2020).

2.2 Aportes académicos en contabilidad y auditoría

2.2.1 Introducción

La producción académica reciente sobre blockchain en contabilidad y auditoría públicas combina promesas de verificación continua con cautelas prácticas sobre gobernanza y adecuación normativa. Diversos trabajos sitúan el aporte central en trasladar el foco “del examen ex post de muestras a la prueba continua sobre poblaciones y reglas del sistema”, con efectos en oportunidad y cobertura del aseguramiento (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). En América Latina, reseñas y tesis de posgrado convergen en que los beneficios dependen de la disciplina de datos, la gobernanza de consorcios y la profesionalización de equipos (Morales, 2021; Santos, 2022; González González, 2023; Luna González Becerril, 2020; Yazuma Carrillo, 2023; Cambo Chillo, 2022; Polimandi, 2023).

En la línea “beneficios–viabilidad”, la evidencia académica perfila un terreno intermedio: blockchain puede reforzar integridad, trazabilidad y auditabilidad si se diseñan metadatos públicos, huellas criptográficas y controles ex ante, pero no sustituye estándares ni políticas (Morales, 2021; Santos, 2022). Este matiz se ve con claridad en tesis que evalúan factibilidad en finanzas públicas: se argumenta la mejora en transparencia y control “si se resuelven cuellos de adopción y se normalizan los datos” (González González, 2023). En contraste, un estudio de caso sobre iniciativas mexicanas advierte que “la implementación [...] no ha alcanzado el alcance esperado” por brechas de digitalización y arreglos institucionales inmaduros (Luna González Becerril, 2020).

La discusión “transparencia–evidencia” se ha enriquecido con trabajos que comparan auditoría tradicional versus auditoría apoyada en libro distribuido y repositorios de documentos. Un hallazgo recurrente es que la combinación registro–hash–sello de tiempo acelera rastreabilidad y cadena de custodia cuando el pipeline de datos está gobernado (Cambo Chillo, 2022). Aun así, la literatura recuerda que la inmutabilidad “congela” inconsistencias si antes no se normalizan catálogos y reglas de negocio (Schmitz & Leoni, 2019; Santos, 2022). La Tabla 3 sintetiza estas contribuciones en una matriz comparativa de tesis y artículos, destacando objetivos, enfoques metodológicos y hallazgos clave.

Tabla 3*Matriz comparativa de tesis y artículos*

Autor	Tipo	Hallazgo/aporte	Condición habilitante	Transf.
Dai & Vasarhelyi (2017)	Artículo	Auditoría/aseguramiento continuo y evidencia reproducible	Gobernanza + diseño de datos + artefactos verificables	Alta
Schmitz & Leoni (2019)	Artículo	Valor condicionado; “inmutabilidad congela errores” si falta normalización	Semántica común + on/off-chain claro	Alta
Grigg (2005)	Paper	Concepto de triple entrada como comprobante compartido	Semántica + integridad criptográfica	Media
Morales (2021)	Artículo	Impacto en contabilidad/auditoría; cambios en riesgo y controles	Capacidades profesionales + gobierno de datos	Media
Santos (2022)	Tesis/Tra bajo	Condiciones y límites de adopción; marco contable	Normativa + estándares + competencias	Media
Cambo Chillo (2022)	Tesis	Evidencia/cadena de custodia con blockchain + repositorio	Proceso reproducible + custodia	Media
Luna González Becerril (2020)	Tesis	Brechas institucionales/digitales limitan impacto real	Madurez digital + gobernanza	Media
González González (2023)	Tesis	Beneficios medibles si hay estándares/métricas	Indicadores + disciplina de datos	Alta
Yazuma Carrillo (2023)	Tesis	Prospectiva en contratación pública al 2030	Secuencia de madurez + regulación	Media

Nota. Elaboración propia a partir de Dai y Vasarhelyi (2017); Schmitz y Leoni (2019); Grigg (2005); Morales (2021); Santos (2022); Cambo Chillo (2022); Luna González Becerril (2020); González González (2023); Yazuma Carrillo (2023).

Una segunda tensión recorre “marco legal–gobernanza tecnológica”: diagnósticos prospectivos en contratación pública subrayan que el salto a producción exige lineamientos de publicación responsable, custodia de llaves y procedimientos de cambio auditables, además de una base normativa que reconozca la fuerza probatoria de artefactos criptográficos (Yazuma Carrillo, 2023). Este encuadre dialoga con revisiones

que explican por qué iniciativas sin estándares claros terminan ralentizadas (Luna González Becerril, 2020) y con estudios que ubican el valor en reglas y procesos más que en la herramienta per se (Santos, 2022).

Un tercer eje es “rol profesional–capacidades”: la literatura especializada insiste en que contadores y auditores deben incorporar lectura de trazas on-chain, lógica de contratos inteligentes y fundamentos criptográficos para traducir artefactos técnicos en evidencia suficiente y apropiada (Morales, 2021; Polimandi, 2023).

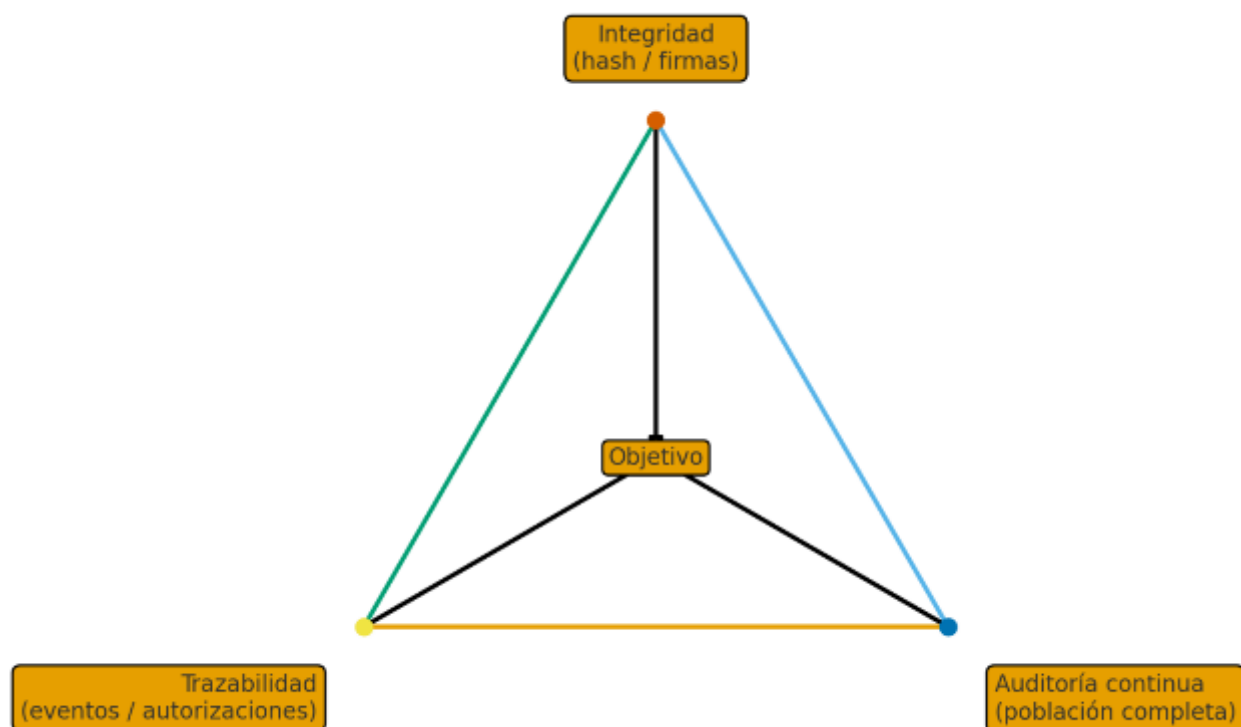
El estado del arte académico llega actualmente a un consenso operativo: blockchain aporta cuando se integra a sistemas de control y de datos bien gobernados, con métricas que prueban reducción de tiempos de auditoría, mejora de conciliaciones y verificabilidad pública de integridad (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019; Morales, 2021).

2.2.2 Convergencias conceptuales: integridad, auditabilidad y “triple entrada”

La literatura reciente converge en un triángulo de valor: integridad criptográfica del registro (hashes y firmas), trazabilidad de eventos y autorizaciones, y posibilidad de auditoría continua sobre poblaciones completas en lugar de muestreos ex post (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). En términos contables, la “triple entrada” incorpora un comprobante compartido que actúa como tercer asiento verificable y reduce conciliaciones, siempre que el diseño semántico y la gobernanza de datos sean consistentes (Grigg, 2005; Santos, 2022). El efecto operativo esperado se resume en menos retrabajo y verificaciones más oportunas basadas en evidencia técnica reproducible (Morales, 2021). La Figura 3 presenta este triángulo de valor en contabilidad pública, articulando integridad, oportunidad y transparencia como ejes para evaluar el aporte de blockchain.

Conviene aclarar, sin embargo, que en el contexto de esta propuesta la referencia a contabilidad de triple entrada no debe interpretarse como una sustitución de los principios contables vigentes ni de los sistemas formales de registración reconocidos por la normativa argentina. La noción se adopta aquí en un sentido técnico-funcional, esto es, como una capa complementaria de evidencia compartida y verificable que refuerza la trazabilidad, la integridad y la auditabilidad de los registros, sin desplazar las reglas contables, presupuestarias y de control que continúan organizando la actuación administrativa del sector público. Esta precisión resulta consistente, además, con el propio estado del arte relevado en el trabajo, donde se sostiene que blockchain puede reforzar integridad, trazabilidad y auditabilidad, pero no sustituye estándares ni políticas.

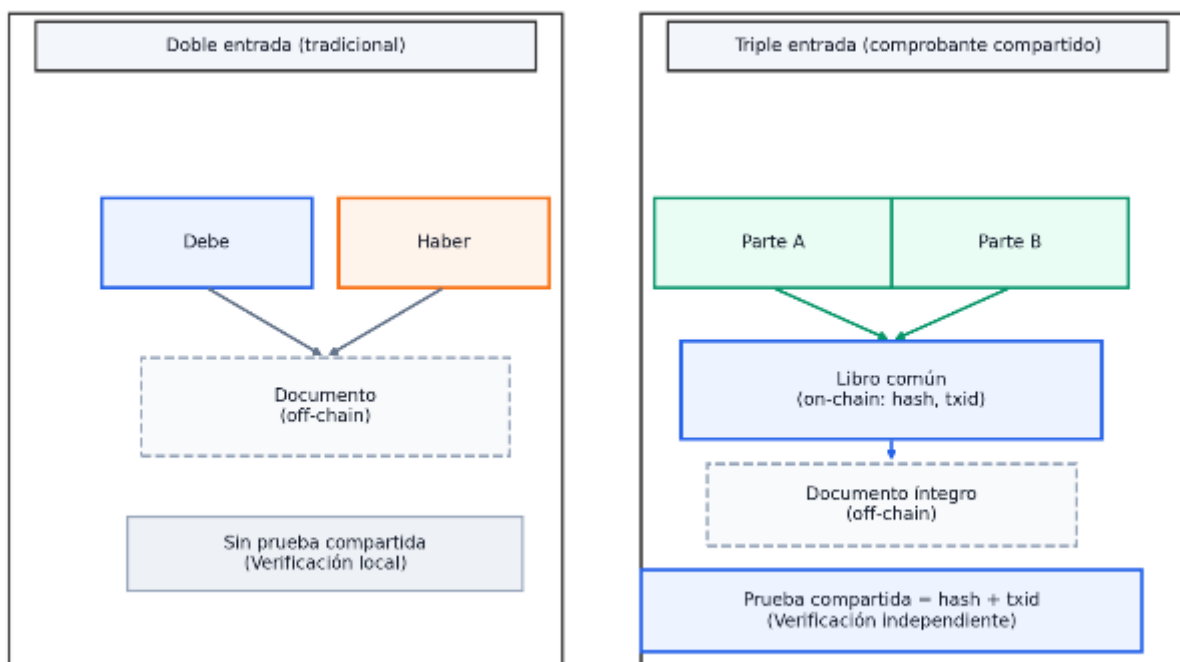
Figura 3
Triángulo de valor en contabilidad pública



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Dai y Vasarhelyi (2017) y Schmitz y Leoni (2019).

La Figura 4 compara la contabilidad de doble entrada tradicional con la propuesta de triple entrada soportada en blockchain, incorporando un comprobante criptográfico compartido.

En la base técnica de la integridad, la literatura fundacional recuerda que “a record that cannot be changed without redoing the proof-of-work” eleva el costo de reversión y fortalece la prueba de no alteración (Nakamoto, 2008, p. 3). Plataformas de propósito general se conciben como “a secure decentralised generalised transaction ledger”, lo que permite trasladar reglas de negocio al propio libro compartido y observar sus eventos para fines de auditoría (Wood, 2014, p. 1). En el plano de aseguramiento, el foco se desplaza hacia pruebas continuas sobre reglas y flujos, y hacia la reproducibilidad de artefactos (hashes, pruebas de inclusión, logs), más que a la revisión puntual de documentos (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019).

Figura 4*Doble entrada vs. triple entrada*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Grigg (2005) y Santos (2022).

En trabajos aplicados recientes, el consenso se matiza con condiciones habilitantes: la triple entrada funciona cuando hay catálogos normalizados, gobierno de claves e identidades y publicación responsable de metadatos y huellas (Santos, 2022; Morales, 2021). Sin pipeline de calidad y semántica común, la inmutabilidad tiende a “congelar” inconsistencias y dificultar su corrección posterior; la ganancia de trazabilidad depende de la disciplina de datos y del mapeo claro on/off-chain (Schmitz & Leoni, 2019; Santos, 2022). Este enfoque se vincula con el giro hacia auditoría continua: pruebas sobre el diseño y la operación del sistema (contratos, identidades, reglas), con métricas de latencia de publicación, porcentaje de asientos con hash verificable y capacidad de reconstruir la cadena de custodia (Dai & Vasarhelyi, 2017). La Tabla 4 detalla los principales artefactos de evidencia y los procedimientos de auditoría asociados en entornos con libro distribuido.

Tabla 4*Artefactos de evidencia y procedimientos de auditoría*

Artefacto	Objetivo	Prueba (reproducible)	Resultado esperado
Hash de documento	Integridad / no alteración	Recalcular hash y cotejar con el publicado on-chain.	Coincidencia exacta.
Prueba de inclusión (Merkle)	Existencia / completitud	Verificar ruta hasta la raíz y el encabezado del bloque.	Ruta válida en el bloque.
Log de evento de contrato	Autorización / secuencia	Leer eventos y reconstruir aprobaciones (quién/cuándo/regla).	Trazabilidad acorde a roles/umbrales.
Sello de tiempo (timestamp)	Oportunidad / existencia en fecha	Comparar marca temporal con hitos del proceso.	Ventanas de tiempo cumplidas.
Firma digital	Autenticidad / no repudio	Validar certificado/cadena y la firma sobre el mensaje.	Firma válida y no revocada.
Conciliación on-chain vs ERP	Exactitud / completitud inter-sistemas	Conciliar estados y montos entre libro distribuido y sistema fuente.	Sin discrepancias materiales (o justificadas).

Nota. Elaboración propia a partir de Dai y Vasarhelyi (2017) y Schmitz y Leoni (2019).

El triángulo de valor se concreta cuando: (a) cada transacción deja un comprobante criptográfico compartido (tercer asiento) que referencia el documento íntegro; (b) las autorizaciones y cambios se registran como eventos verificables con firma y sello de tiempo; y (c) la auditoría migra a pruebas continuas sobre datos normalizados y reglas de control, con métricas de cobertura y oportunidad. De lo contrario, la inmutabilidad solo fija inconsistencias y traslada el problema a otra capa.

La convergencia conceptual no reside en “poner todo en cadena”, sino en articular triple entrada, publicación mínima verificable y auditoría continua sobre un sistema auditable. La contribución de este trabajo se alinea con esa estructura: operacionalizar el tercer asiento mediante metadatos y huellas y medir su impacto en tiempos de auditoría, conciliaciones y verificabilidad pública de la integridad. La Tabla 5 resume las condiciones habilitantes para que la contabilidad de triple entrada resulte útil en el sector público.

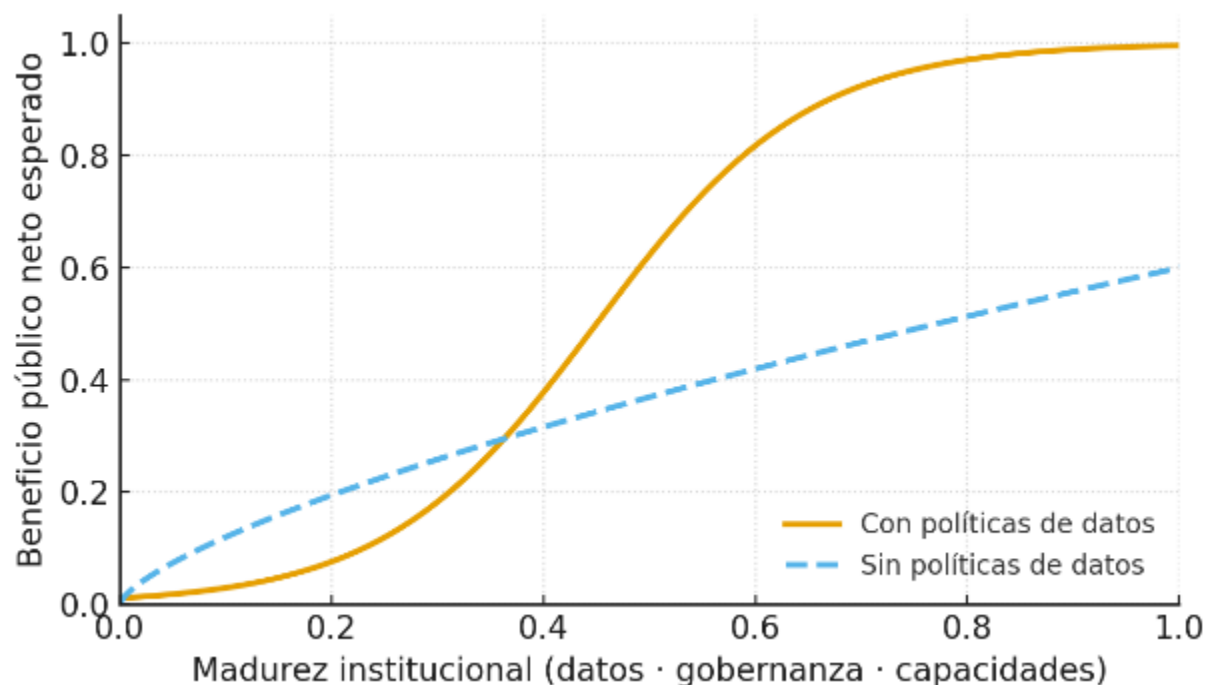
Tabla 5
Condiciones habilitantes para triple entrada útil

Condición	Qué exige	Métrica sugerida	Riesgo si falta
Datos (diccionarios/ versionado)	Catálogos cerrados, esquemas versionados y linaje.	% de registros con metadatos completos/validados.	Inconsistencias inmutables; conciliación inviable.
Gobernanza (claves/roles)	Custodia en HSM/MPC, MFA, SoD y umbrales.	% de operaciones críticas con multifirma y revisión periódica.	Firmas indebidas o pérdida de claves; sin trazabilidad.
Publicación (metadatos mínimos)	ID, hash, timestamp y estado; documentos íntegros off- chain.	% de asientos con hash verificable y enlace a documento.	Evidencia insuficiente o filtración de datos.
Métricas operativas	Medir latencia, discrepancias on/off-chain y cobertura de controles.	p95 de latencia; discrepancias/1000; % con control ex ante.	No demostrar eficiencia ni calidad de control.

Nota. Elaboración propia a partir de Santos (2022) y Morales (2021).

2.2.3 Viabilidad económico-social vs. límites de adopción

El bloque reciente de tesis de posgrado en la región muestra una tensión clara: la promesa de beneficios económicos y sociales frente a los costos y fricciones de adopción. Desde una visión propositiva, se sostiene que una arquitectura orientada a finanzas públicas puede generar ahorros operativos y externalidades de transparencia si la adopción se acompaña de estándares, métricas y políticas de publicación responsable (González González, 2023). A la vez, estudios de caso registran que, aun cuando el potencial técnico es claro, las brechas de digitalización, gobernanza y capacidades pueden impedir que los proyectos alcancen el alcance esperado (Luna González Becerril, 2020). Esta lectura coincide con el consenso internacional: el valor no emana del on-chain per se, sino de cómo se gobiernan datos, roles y cambios, y de si la evidencia generada es suficiente y apropiada para auditoría (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; International Organization of Supreme Audit Institutions [INTOSAI], 2013). La Figura 5 representa de forma conceptual la curva de beneficio público en función del nivel de madurez de adopción de blockchain en finanzas públicas.

Figura 5*Curva beneficio público vs. madurez de adopción*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en González González (2023) y Luna González Becerril (2020).

En clave económico-social, la evaluación de conveniencia no puede reducirse a la tecnología. La tesis de referencia mexicana plantea un balance entre beneficios públicos (trazabilidad, reducción de costos de verificación, menor discrecionalidad) y costos de adopción (interoperabilidad, resguardo de claves, operación 24x7), proponiendo anclar la decisión en indicadores verificables y reglas de datos explícitas (González González, 2023). En contraste empírico, un estudio de iniciativa pública en México concluye que la madurez institucional y digital condiciona el impacto: sin catálogos normalizados, procedimientos de cambio y responsabilidades trazables, la inmutabilidad fija inconsistencias y desplaza el problema (Luna González Becerril, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Un corolario transversal es el rol profesional. La formación contable y de auditoría resulta decisiva para traducir artefactos técnicos (hashes, pruebas de inclusión, logs de eventos) en evidencia probatoria, rediseñar pruebas y sostener controles programables. Como sintetiza una tesis argentina, el contador y el auditor se vuelven “participante clave en la fiabilidad de la información contable” (Polimandi, 2023, título). Este énfasis dialoga con el giro metodológico hacia auditoría continua propuesto por la literatura internacional, que desplaza el foco desde el muestreo ex post hacia la evaluación del diseño y la operación

del sistema (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). La Tabla 6 organiza estos factores en una matriz de decisión de adopción, relacionando riesgos, capacidades y condiciones habilitantes.

Tabla 6

Matriz de decisión de adopción

Área	Pregunta de umbral	Evidencia requerida	Riesgo no cumpl.	Métrica de salida
Datos	¿Hay diccionarios y esquemas comunes y versionados?	Diccionario; esquemas; actas; repo Git	Inconsistencias on/off-chain; errores inmutables	% asientos con hash; latencia (min)
Gobernanza	¿Están definidos membresía, quórum y segregación?	Estatuto; RACI; votos; actas firmadas	Discrecionalidad; falta de no repudio; bloqueos	% cambios con quórum; aprobación (días)
Claves/Identidades	¿Política HSM/MPC con rotación, revocación y MFA?	Política de claves; bitácoras HSM; rotación/revocación; restauración	Firmas indebidas; pérdida de autoría; incidentes	Cobertura MFA (%); incidentes; rotación (días)
Operación/Desempeño	¿Pruebas de capacidad/latencia y SLO de finalidad/cierre?	Cargas; reportes de latencia; parámetros; monitoreo	Finalidad incierta; reversiones; cuellos de botella	Finalidad (s); disponibilidad (%); ERP→on-chain (s/min)
Normativa/Evidencia	¿Mapeo on/off-chain conforme a acceso a la info y PD?	Matriz legal; políticas; hash/timestamp; cadena de custodia	Exposición de datos; evidencia no admisible	% artefactos con hash; respuesta (días)

Nota. Elaboración propia a partir de Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); International Organization of Supreme Audit Institutions (2013); Schmitz y Leoni (2019).

En términos de decisión pública, los hallazgos apuntan a ordenar la adopción por etapas, con métricas de resultado y gobierno de datos. La evidencia comparada sugiere pilotear con indicadores de eficiencia y trazabilidad, fijar políticas de claves e identidades y publicar metadatos y huellas verificables sin exponer contenido sensible (González González, 2023; Luna González Becerril, 2020). La viabilidad económico-social de blockchain en contabilidad pública depende de un “paquete” institucional: datos gobernados y normalizados, controles programables revisados de manera independiente, publicación

mínima verificable y capacidades profesionales para sostener auditoría continua. Cuando ese paquete está ausente, los límites de adopción superan los beneficios; cuando está presente, la tecnología se convierte en un medio mensurable para reducir tiempos de auditoría, mejorar la trazabilidad y fortalecer la rendición de cuentas (González González, 2023; Luna González Becerril, 2020; Polimandi, 2023; Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019).

2.2.4 Prospectiva en compras públicas

La prospectiva académica reciente coincide en que el potencial anticorrupción de blockchain en contrataciones depende de habilitantes institucionales y legales, además del diseño técnico (Yazuma Carrillo, 2023). Los escenarios al 2030 más verosímiles incluyen secuencias graduales: estandarización de datos de compra, reglas de publicación y resguardo de evidencias, automatización de controles ex ante y, recién después, escalamiento a dominios adyacentes (Yazuma Carrillo, 2023; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Esta línea dialoga con la literatura internacional que traslada el foco desde “escribir en cadena” hacia gobernar datos, membresías y quórums con métricas reproducibles (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019).

Los casos revisados son consistentes en un punto: la ganancia de transparencia solo es sostenible si la publicación es responsable. Ello implica metadatos verificables y huellas criptográficas en la red, documentos íntegros en repositorios con control de acceso y trazabilidad de transformaciones entre sistemas (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Una tesis latinoamericana resume el beneficio como contingente a “políticas, estándares y métricas” que reduzcan asimetrías de información y objetiven el desempeño (González González, 2023), mientras análisis empíricos subrayan los límites de adopción cuando el “entorno digital” y la gobernanza son insuficientes para sostener pilotos más allá de la demostración (Luna González Becerril, 2020).

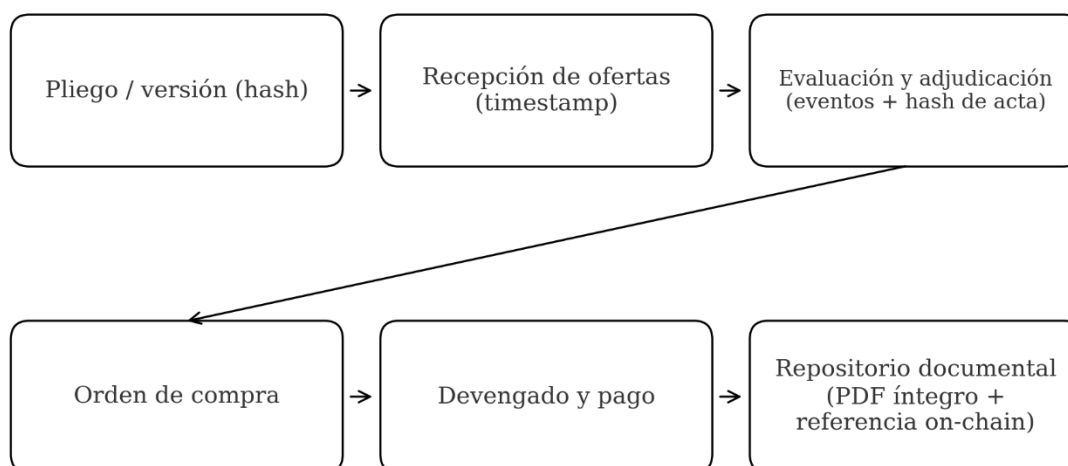
Los enfoques de aseguramiento continuo proponen medir, en compras, cuatro frentes: oportunidad (latencia orden→adjudicación→pago), alcance (porcentaje de eventos con hash verificable), consistencia (discrepancias on/off-chain) y trazabilidad (existencia de pruebas de inclusión) (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). Sobre esa base, la recomendación es explicitar “quién valida, con qué reglas y bajo qué responsabilidad” antes de automatizar, para evitar que la inmutabilidad consolide inconsistencias (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Yazuma Carrillo, 2023).

En clave de adopción, la literatura propone sandboxes o betas regulatorias que permitan probar con métricas y salvaguardas antes de escalar (González González, 2023; Yazuma Carrillo, 2023). Una formulación breve lo resume como “probar bajo control, medir con estándares y publicar con resguardo”: los incentivos de los actores y la gobernanza de claves/membresías condicionan el resultado (Foro

Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Figura 6 sintetiza la cadena de evidencia en procesos de compras públicas con publicación responsable.

Figura 6

Cadena de evidencia en compras con publicación responsable



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Foro Económico Mundial & Banco Interamericano de Desarrollo (2020) y Schmitz y Leoni (2019).

La ruta de diseño para compras públicas con fines de transparencia y control se orienta por tres principios: datos y semánticas estandarizados que habiliten publicación responsable; controles ex ante programables con evidencias criptográficas reproducibles; y validación regulatoria con métricas de resultado que hagan transferible el piloto a otras jurisdicciones (Yazuma Carrillo, 2023; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). El valor no surge del on-chain per se, sino del ensamblaje entre gobernanza, datos y medición.

2.2.5 Evidencia y cadena de custodia

La literatura coincide en que el valor probatorio de blockchain no reside en “escribir en cadena”, sino en cómo se estandarizan metadatos, se gobierna la publicación responsable (on/off-chain) y se preserva

la cadena de custodia de extremo a extremo (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). Un estudio comparativo que contrasta auditoría tradicional con un esquema blockchain + IPFS reporta mejoras en oportunidad de verificación y trazabilidad, condicionadas a normalización semántica y reglas claras sobre qué se publica en la red y qué se resguarda fuera (Cambo Chillo, 2022). Esta línea dialoga con la doctrina de aseguramiento sobre sistemas: artefactos como hashes de documentos, marcas de tiempo, pruebas de inclusión (Merkle) y logs de eventos se vuelven equivalentes funcionales de sellos y firmas, siempre que su obtención y custodia sean reproducibles por terceros (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019).

Desde el control, se recuerda que el auditor sigue obligado a reunir “evidencia suficiente y apropiada”, por lo que la arquitectura técnica debe garantizar confiabilidad de fuentes, trazabilidad de transformaciones y documentación del trabajo (International Organization of Supreme Audit Institutions [INTOSAI], 2013, seccs. 43–45). En términos operativos, el pipeline probatorio incluye: (a) cálculo del hash sobre el documento íntegro y registro de su huella; (b) anclaje on-chain de metadatos mínimos (identificador, estado, sello de tiempo, hash); (c) resguardo off-chain del original con control de acceso y registros de descarga; (d) verificación independiente mediante recomputación de hash y prueba de inclusión; y (e) bitácoras firmadas de cambios y accesos (Schmitz & Leoni, 2019; Santos, 2022). Cuando estos pasos fallan, la inmutabilidad solo “congela” errores previos; cuando se cumplen, habilitan auditoría continua con analítica sobre población completa (Morales, 2021).

En el contraste empírico, los estudios observan que la “atmósfera de transparencia” surge cuando cada evento clave del ciclo queda instrumentado con evidencias verificables (Cambo Chillo, 2022). El plus probatorio proviene de la posibilidad de reejecutar verificaciones (recalcular hashes, seguir rutas Merkle, reconstruir autorizaciones desde eventos) y de reproducir la cadena de custodia, no de la tecnología aislada (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). Sobre esta base se proponen criterios de medición: completitud (porcentaje de transacciones con hash verificable), oportunidad (latencia documento→anclaje), consistencia (discrepancias on/off-chain) y trazabilidad (existencia de prueba de inclusión por muestra o por universo) (Dai & Vasarhelyi, 2017; Morales, 2021). La Tabla 7 presenta una matriz on-chain/off-chain para evidencia contable.

Tabla 7*Matriz on-chain/off-chain para evidencia contable*

Elemento	Sensibilidad	Ubicación	Artefacto probatorio	Prueba de verificación	Responsable	Retención
ID de asiento (UUID)	Baja	On-chain	TxID + hash	Comparar hash con registro	Contabilidad	Permanente
Fecha y tipo de operación	Baja	On-chain	Timestamp on-chain	Verificar marca de tiempo	Contabilidad	Permanente
Estado de aprobación (workflow)	Media	On-chain	Evento de contrato	Leer event logs	Tesorería/Compras	Histórico
Hash de documento soporte (PDF)	Alta	On-chain	Hash + Merkle	Re-hash + prueba de inclusión	Archivo/Legales	Según norma
Documento soporte (PDF íntegro)	Alta	Off-chain	Repositorio con control de acceso	Abrir documento y validar hash	Archivo/Legales	Según archivo
Identificador de proveedor (CUIT)	Alta	Off-chain	Registro IAM	Cruce con catálogo	Compras/Datos	Según DP
Firma/Certificado digital	Alta	Off-chain	PKI/HSM	Validar cadena y vigencia	Seguridad TI	Según Ley 25.506
Registro de accesos/descargas	Media	Off-chain	Logs firmados	Revisión de bitácoras	TI/Auditoría	Según política

Nota. Elaboración propia a partir de Dai y Vasarhelyi (2017); Schmitz y Leoni (2019); International Organization of Supreme Audit Institutions (2013).

Las aportaciones académicas de la región proponen una regla operativa: separar metadatos y huellas (publicables) de documentos íntegros (resguardados), normalizar el significado contable y diseñar verificaciones reproducibles por terceros. Solo entonces la inmutabilidad técnica se traduce en evidencia útil y en costos de auditoría decrecientes (Cambo Chillo, 2022; Morales, 2021; Santos, 2022).

2.2.6 Competencias profesionales y aseguramiento sobre sistemas

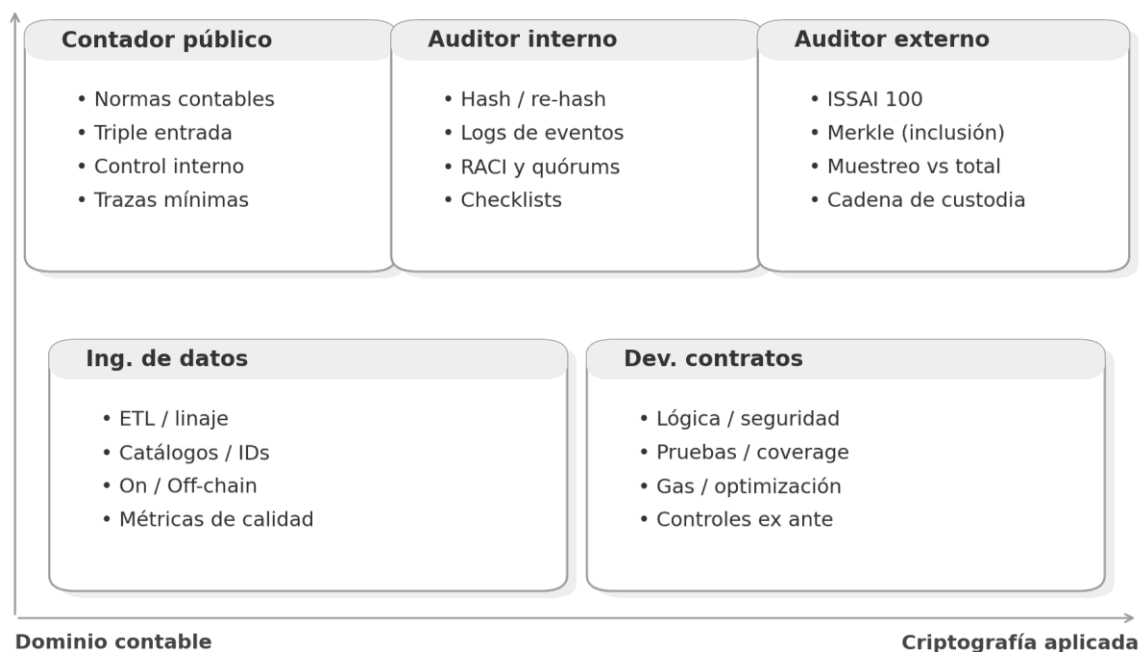
La producción reciente es consistente en un punto: la promesa de integridad y auditabilidad solo se concreta si el perfil profesional incorpora lectura de trazas on-chain, verificación de artefactos criptográficos, revisión de contratos inteligentes y gobierno de claves/identidades, con procedimientos de aseguramiento sobre sistemas (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019; Santos, 2022). Ello desplaza el foco desde “auditar saldos” hacia “auditar el sistema que genera los saldos”, rearticulando pruebas sustantivas y de cumplimiento con analítica continua y replicabilidad de evidencia (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). En América Latina, varias tesis advierten que, sin formación específica y arreglos institucionales, los beneficios se diluyen o quedan restringidos a pilotos (Luna González Becerril, 2020; Polimandi, 2023).

En términos de funciones, el campo converge en un repertorio mínimo de competencias: modelado de datos y semántica contable para on/off-chain, inspección de contratos (segregación de funciones, umbrales de aprobación, control de cambios), pruebas de reejecución determinista y trazabilidad de cadena de custodia (Santos, 2022; Schmitz & Leoni, 2019). Esto reclama planes de capacitación con doble eje: dominio contable/normativo y alfabetización criptográfica/protocolar, además de prácticas de laboratorio con datasets sintéticos y entornos de preproducción (Dai & Vasarhelyi, 2017; Santos, 2022). Como subraya una tesis reciente, el profesional pasa a ser “participante clave en la fiabilidad de la información contable” (Polimandi, 2023, p. 1). La Figura 7 resume estas capacidades en un mapa de competencias para auditoría en entornos blockchain.

En el plano del aseguramiento, el estándar normativo se mantiene: la evidencia debe ser suficiente y apropiada, con criterios y documentación que permitan la comprensión por otro auditor competente (INTOSAI, 2013). Por ello, la literatura propone traducir artefactos técnicos a programas de trabajo: recalcular hashes y contrastarlos con publicaciones on-chain; verificar inclusión en árboles de Merkle; reconstruir aprobaciones desde eventos; y conciliar on/off-chain por población o por muestra de alto riesgo (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019). El control interno aporta la matriz de diseño (ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, monitoreo), que en blockchain se traduce en políticas de claves y multifirma, RACI de cambios, observabilidad de nodos y auditorías periódicas de contratos (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013). La Tabla 8 detalla la relación entre competencias requeridas y actividades de aseguramiento.

Figura 7

Mapa de competencias para auditoría en entornos blockchain



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Schmitz y Leoni (2019), Santos (2022) y Dai y Vasarhelyi (2017).

Vistas en conjunto, las aportaciones académicas latinoamericanas proponen una hoja de ruta para la profesión: definir objetos de evidencia y métricas (porcentaje de asientos con hash verificable, latencia documento→anclaje, discrepancias on/off-chain), instalar capacidades para inspección de contratos y gestión de claves y alinear programas de auditoría con controles embebidos en la red (Luna González Becerril, 2020; Polimandi, 2023; Santos, 2022). Sin ese andamiaje, la inmutabilidad técnica se transforma en “inmutabilidad de errores”; con él, habilita aseguramiento continuo con costos de verificación decrecientes (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019).

Tabla 8*Matriz de competencias vs. actividades de aseguramiento*

Actividad	Evidencia	Criterio de aceptación	Responsable / frecuencia
Hash / re-hash de documento	Hash SHA-256 reproducible que coincide on-chain	Coincidencia exacta y marca temporal válida	Auditoría (int./ext.); por muestra / ad hoc
Prueba de inclusión (Merkle)	Ruta de inclusión válida hasta la raíz publicada	Verifica bloque y transacción objetivo	Auditor ext. / ing. de datos; por lote
Lectura de event logs	Bitácora decodificada (ABI) con firmas y parámetros	Secuencia y autorizaciones coherentes	Auditor int. / dev. de contratos; mensual / cierres
Conciliación on/off-chain	Cuadre ERP/documentos vs. metadatos on-chain	Diferencias $\leq$ umbral; excepciones justificadas	Ing. de datos / contabilidad; mensual / trimestral
Revisión de contratos inteligentes	Informe de hallazgos y controles programados	Sin vulnerabilidades críticas; controles alineados	Dev. de contratos / seguridad / auditoría; pre-despliegue y anual
Gestión de claves y accesos	Actas de rotación, registros HSM, listas de permisos	Segregación de funciones y rotación documentada	Seguridad TI / auditoría interna; trimestral / cambios

Nota. Elaboración propia a partir de Dai y Vasarhelyi (2017); Schmitz y Leoni (2019); International Organization of Supreme Audit Institutions (2013); Committee of Sponsoring Organizations of the Treadway Commission (2013).

2.2.7 Síntesis dialógica y vacíos de investigación

Leída en conjunto, la literatura 2020–2025 perfila un consenso condicionado: blockchain promete integridad verificable y auditoría más oportuna, pero su valor depende de gobernanza de datos, controles sobre sistemas y capacidades profesionales instaladas (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019; Morales, 2021; Santos, 2022). En tesis latinoamericanas recientes, el optimismo técnico convive con evaluaciones prudentes sobre costos de adopción, brechas de digitalización y marcos normativos en ajuste (González González, 2023; Luna González Becerril, 2020; Yazuma Carrillo, 2023; Cambo Chillo, 2022; Polimandi, 2023).

En el plano de resultados, el eje comparativo se desplaza desde el “cumple/no cumple” hacia métricas de desempeño del sistema de registro: oportunidad de evidencia, discrepancias on/off-chain,

cobertura de controles ex ante y trazabilidad de autorizaciones. Mientras que la literatura internacional propone auditoría continua y pruebas reproducibles sobre poblaciones completas (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019), los trabajos locales piden cautela metodológica para evitar tecnosolucionismo y sostener indicadores verificables en contextos con datos heterogéneos y responsabilidades difusas (Luna González Becerril, 2020; Polimandi, 2023). En términos de ruta de adopción, el balance dialógico converge en secuenciar: normalización y gobierno de datos, controles embebidos y, recién después, escalamiento con evaluación costo-beneficio de la auditoría continua (Yazuma Carrillo, 2023; Santos, 2022). La Figura 8 representa un mapa de convergencias y tensiones en la literatura 2020–2025.

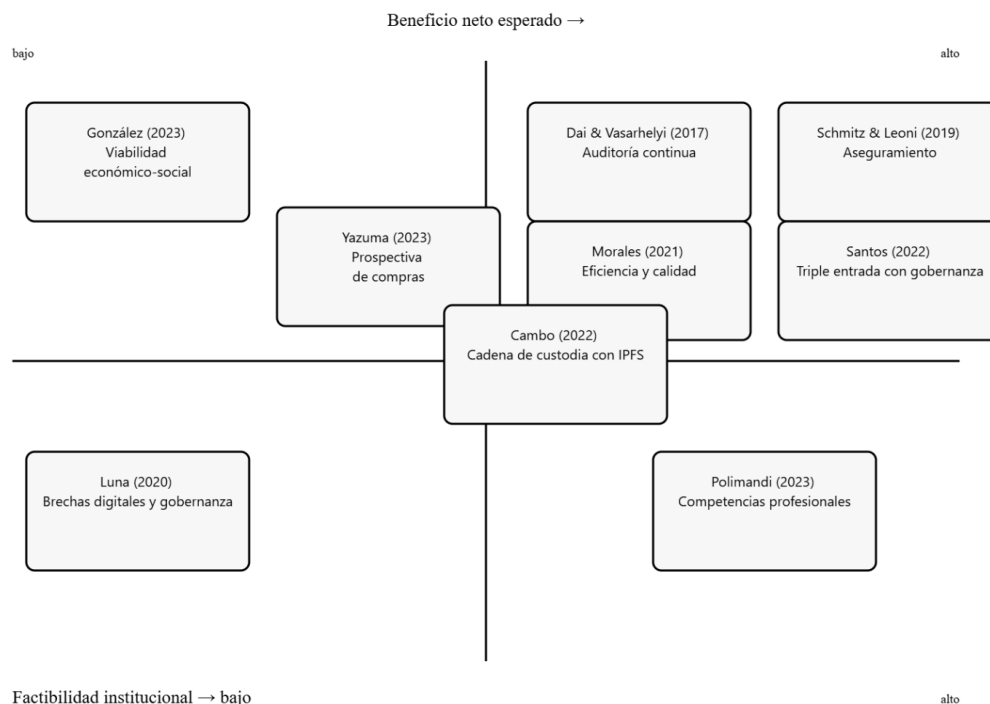
Un clivaje central aparece entre promesa y factibilidad. González González (2023) discute beneficios económicos y sociales en finanzas públicas si existen estándares y métricas operativas; a la vez, un estudio de caso mexicano concluye que iniciativas públicas “no alcanzaron el alcance esperado” por un “entorno digital [...] poco óptimo” y obstáculos institucionales (Luna González Becerril, 2020). La tesis del campo se refuerza: el valor no surge del on-chain per se, sino del diseño institucional que gobierna datos, roles y cambios (Morales, 2021; Santos, 2022).

La Tabla 9 organiza estos desafíos en una agenda de investigación, señalando líneas prioritarias y vacancias metodológicas en contabilidad y auditoría sobre blockchain.

Los vacíos prioritarios para investigación-acción en Argentina pueden sintetizarse en cuatro frentes: (a) estudios cuasi-experimentales sobre procesos contables completos (no solo compras), comparando líneas de base con pilotos híbridos mediante indicadores de tiempo de auditoría, discrepancias on/off-chain y tasa de controles ex ante efectivos (Dai & Vasarhelyi, 2017; Santos, 2022); (b) diseños de gobernanza medibles (membresías, quóruns, gestión de claves) alineados con control interno, con pruebas de efectividad y trazabilidad de cambios (Schmitz & Leoni, 2019; COSO, 2013); (c) evaluación costo-beneficio de auditoría continua en entornos públicos, incluyendo costos de operación, formación y mantenimiento de contratos frente a reducción de conciliaciones y tiempos de respuesta (Morales, 2021; González González, 2023); y (d) programas de capacitación que midan la adquisición de competencias para auditar sistemas distribuidos, desde lectura de eventos hasta reejecución determinista de reglas (Polimandi, 2023; Luna González Becerril, 2020).

Figura 8

Mapa de convergencias y tensiones 2020–2025



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Dai y Vasarhelyi (2017); Schmitz y Leoni (2019); González González (2023); Luna González Becerril (2020).

En conjunto, el estado del arte sostiene una promesa condicionada: blockchain no resuelve por sí sola los problemas de transparencia, pero, bien encuadrada, puede ayudar a abordar déficits de integridad y trazabilidad en el registro público, siempre que la adopción avance con métricas, gobierno de datos y capacidades verificables (González González, 2023; Morales, 2021; Santos, 2022). La contribución de este trabajo se ubica en traducir ese consenso a un diseño evaluable de proceso contable en Argentina, con indicadores replicables y validación probatoria.

Tabla 9
Agenda de investigación

Pregunta / Hipótesis	Diseño	Resultados	Unidad	Fuentes	Validez
¿La publicación verificable reduce la latencia de evidencia?	ITS	Latencia (min); % asientos con hash	Proceso (mensual)	Libro distribuido + ERP + logs	Estacionalidad controlada; hash replicable
¿Los controles embebidos disminuyen discrepancias on/off-chain?	DiD	Tasa de discrepancias; retrabajos	Unidad ejecutora	ERP + eventos on-chain	Control comparable; pruebas de balance
¿La auditoría continua acorta tiempos de cierre?	Cuasi-experimento o por fases	Tiempo de cierre; hallazgos repetidos	Organismo / área piloto	Cronogramas + logs	Cambio único; intervención documentada
¿Mayor % de controles on-chain se asocia con menor riesgo?	Cohorte longitudinal	% con control ex ante; incidentes	Programa / partida	Eventos de contrato + informes de auditoría	Indicadores estables; trazabilidad completa

Nota. Elaboración propia a partir de Dai y Vasarhelyi (2017); International Organization of Supreme Audit Institutions (2013); Santos (2022); Schmitz y Leoni (2019).

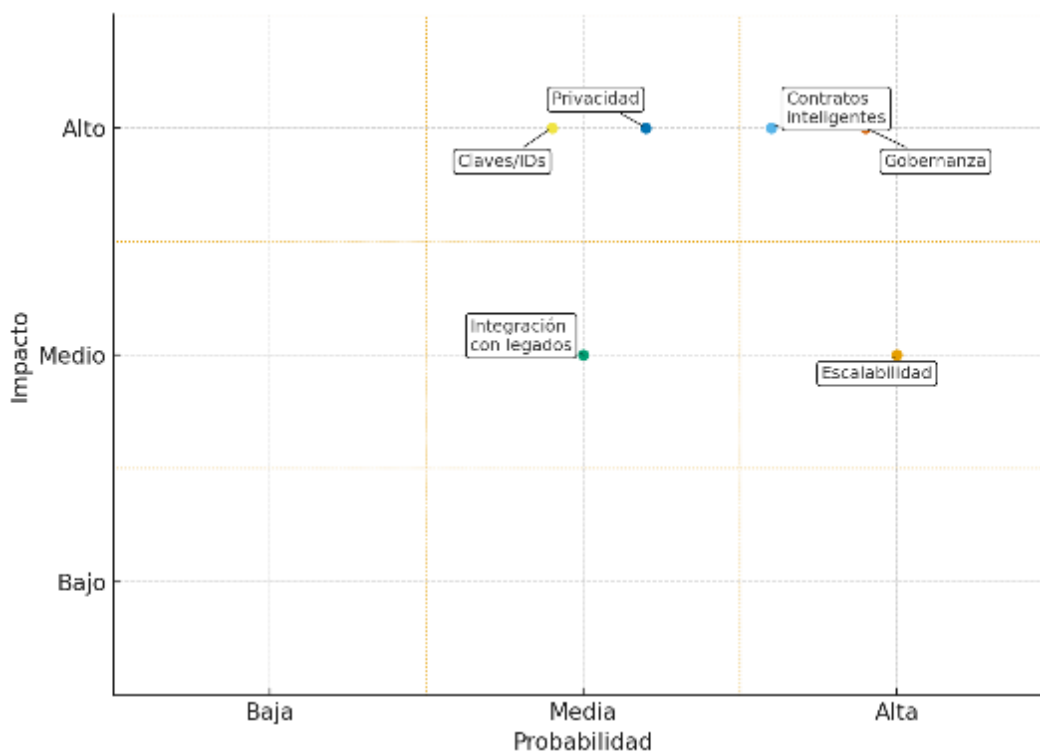
2.3 Riesgos, barreras y marcos de control

La investigación reciente converge en que los beneficios de blockchain para lo público dependen de cómo se gobiernan los riesgos técnicos, organizacionales y normativos. El Banco Interamericano de Desarrollo resume la advertencia con claridad al señalar que la utilidad real surge cuando existen reglas explícitas sobre datos, roles y auditoría, y no de la herramienta por sí misma (Banco Interamericano de Desarrollo [BID], 2020). En la misma dirección, el Foro Económico Mundial y el BID documentan que los proyectos exitosos combinan diseño tecnológico con acuerdos verificables de gobernanza, gestión de

identidades y trazabilidad de responsabilidades a lo largo de todo el ciclo de vida (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

En el plano técnico, la literatura identifica tres focos de riesgo recurrentes. Primero, la escalabilidad y el rendimiento: latencias impredecibles y capacidad limitada pueden obstaculizar cierres contables y conciliaciones temporizadas; la respuesta típica en contextos públicos ha sido optar por redes permissionadas con consenso BFT y anclaje público periódico, equilibrando finalidad rápida y verificabilidad externa (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Segundo, los errores en contratos inteligentes: un fallo lógico puede propagar asientos inválidos a gran velocidad; se recomienda aplicar principios de ingeniería segura, revisión externa y despliegue con multifirma y ventanas de cambio controladas (COSO, 2020). Tercero, la integración con sistemas legados: sin un pipeline de calidad y trazabilidad de orígenes, la cadena solo “congela” inconsistencias previas; normalizar catálogos y documentar reglas antes de programarlas es condición de éxito (BID, 2020). La Figura 9 resume estos riesgos en un mapa de calor, clasificando probabilidad e impacto de los principales focos técnicos en proyectos de blockchain público.

Los riesgos organizacionales y de gobernanza son igualmente determinantes. La gestión de claves y de identidades operativas define quién puede autorizar qué, bajo qué quóruns y con qué evidencia; la difusión de responsabilidades —cuando todos “pueden” pero nadie “responde”— es un patrón de falla descrito tanto por guías sectoriales como por marcos de control interno (BID, 2020; COSO, 2013). Además, la privacidad y la confidencialidad obligan a separar con criterio qué se publica on-chain (metadatos, estados, hashes) y qué permanece off-chain (documentos completos, datos sensibles), combinando técnicas de minimización, cifrado y pruebas de conocimiento cero cuando corresponda (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 10 traduce los riesgos identificados en una matriz riesgo-control inspirada en el marco COSO, vinculando amenazas específicas con actividades de control propuestas.

Figura 9*Mapa de calor de riesgos*

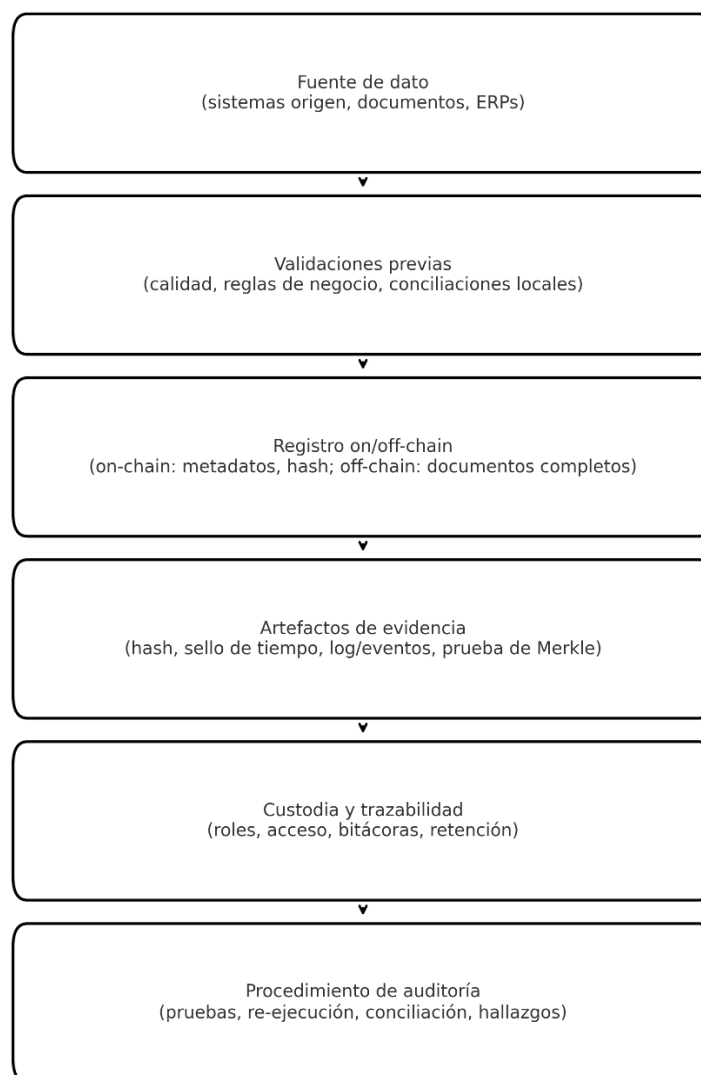
Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Desde el control interno, el marco COSO resulta el ancla para traducir riesgos a controles. En su versión general, establece cinco componentes interdependientes —ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y monitoreo— que orientan la asignación de responsabilidades, la segregación de funciones y la supervisión continua (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013). Su guía específica sobre blockchain enfatiza que la tecnología puede reforzar controles preventivos y detectivos, pero también incorpora riesgos nuevos que obligan a definir políticas de membresía, gestionar formalmente los cambios, monitorear contratos y nodos, y establecer métricas de efectividad (COSO, 2020). En síntesis, COSO (2020) remarca que ninguna tecnología reemplaza a la gobernanza: los controles deben estar diseñados y operar con suficiente evidencia, independencia y trazabilidad como para cumplir los objetivos de información y de cumplimiento (p. 6). La Figura 10 esquematiza el flujo de evidencia aceptable según la ISSAI 100, desde la generación de registros hasta su uso en conclusiones de auditoría.

Tabla 10*Matriz riesgo-control (enfoque COSO)*

Riesgo	Componente COSO	Preventivo	Detectivo	Evidencia	Responsable
Escalabilidad	Actividades de control	Capacidad planificada; límites; pruebas de carga	Monitoreo de desempeño y alertas	Logs y métricas; actas de pruebas	Infraestructura / TI
Error de control inteligente	Evaluación de riesgos	Pruebas de controles de negocio	Monitoreo de código y eventos	Evidencia de pruebas; eventos; logs	Arquitectura / Seguridad TI
Integración con legados	Información y comunicación	APIs firmadas; validaciones en proceso	Conciliaciones periódicas de datos	Bitácoras ETL; reportes/errores	Desarrollo / TI
Claves e identidades	Ambiente de control	HSM/multifirma; segregación; accesos	Auditorías de acceso; rotación de claves	Registros HSM; actas de rotación; trazas	Seg. de la información / RR. HH.
Privacidad	Evaluación de riesgos	Clasificación; cifrado; control de acceso	Pruebas de filtrado; revisión de accesos	Matrices; logs de consulta; informes	Datos / Legales
Responsabilidad de decisiones	Monitoreo	Revisión de decisiones; conciliaciones	Verificación de actas y conciliaciones	Actas; informes de conciliación	Gobernanza / Auditoría interna

Nota. Adaptado de Committee of Sponsoring Organizations of the Treadway Commission (2013, 2020).

Figura 10*Flujo de evidencia aceptable según ISSAI 100*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en International Organization of Supreme Audit Institutions (2013).

Por su parte, la auditoría del sector público aporta los criterios de validez probatoria. La ISSAI 100 recuerda que el auditor debe obtener “evidencia suficiente y apropiada” para sustentar sus conclusiones, considerando la confiabilidad de las fuentes y la oportunidad de los registros (International Organization of Supreme Audit Institutions [INTOSAI], 2013). Trasladado a blockchain, el debate se centra en qué artefactos son aceptables —hashes, sellos de tiempo, logs de eventos, pruebas de Merkle—, cómo se obtienen sin vulnerar restricciones legales y quién custodia las claves y los repositorios asociados.

Blockchain solo es viable en contabilidad pública cuando se articula con una gobernanza explícita de datos y de consorcio, controles de roles y de cambios compatibles con COSO, y validación regulatoria de la evidencia producida según ISSAI 100. Las barreras técnicas —escalabilidad, errores en contratos, integración— y las de gobernanza —claves, privacidad, responsabilidades— deben abordarse ex ante mediante diseño de controles, políticas y procedimientos medibles; de lo contrario, la inmutabilidad solo consolidará problemas preexistentes (BID, 2020; COSO, 2013, 2020; INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 11 sintetiza estos requisitos en un checklist de gobernanza para redes permissionadas, combinando aspectos de consorcio, datos y control interno.

Tabla 11
Checklist de gobernanza (redes permissionadas)

Aspecto	Ítem de verificación
Membresía y quórum	Criterios de admisión/expulsión; quórum definidos (p. ej., 2/3) para cambios
Gestión de claves	Uso de HSM/multifirma; rotación y recuperación documentadas; no
Change management	Proceso formal de propuesta–revisión–aprobación–despliegue; revisiones y versión segura;
Monitoreo continuo	Métricas, logs y alertas; auditorías periódicas de nodos/contratos; planes de
Privacidad por diseño	Clasificación de datos; minimización on-chain; controles de acceso; pruebas
Plan de incidentes	Runbooks, responsabilidades y lecciones aprendidas; simulacros y reciclones

Nota. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); Committee of Sponsoring Organizations of the Treadway Commission (2013, 2020); International Organization of Supreme Audit Institutions (2013).

2.4 Iniciativas y evidencias en América Latina

2.4.1 Introducción

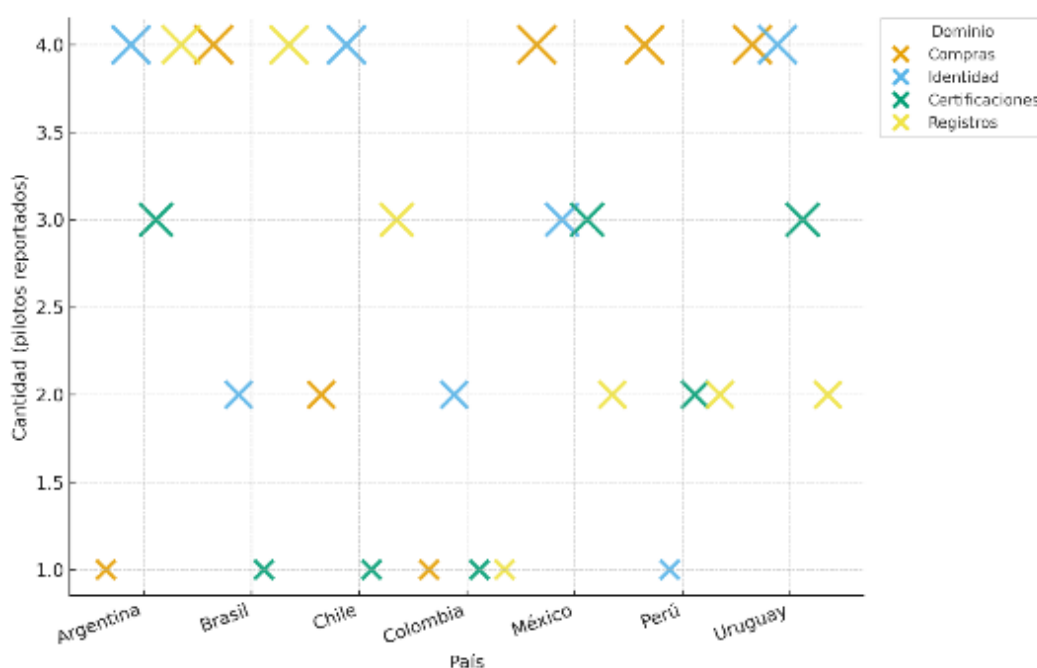
La experiencia latinoamericana muestra que blockchain aporta valor público cuando se inserta en arreglos de gobernanza interinstitucional, reglas de datos explícitas y controles compatibles con los marcos de control interno y de auditoría; fuera de ese encuadre, la inmutabilidad tiende a cristalizar inconsistencias

heredadas. El Banco Interamericano de Desarrollo describe la tecnología como infraestructura habilitante para procesos de gobierno abierto y auditoría verificable, con énfasis en trazabilidad de estados y preservación de confidencialidad mediante separación on/off-chain (Banco Interamericano de Desarrollo [BID], 2020).

En esta línea, las recomendaciones regionales proponen focalizar en dominios con externalidades públicas claras (compras y contrataciones, certificaciones, identidad), definiendo desde el inicio qué metadatos se publican, qué evidencias criptográficas se conservan y qué documentos permanecen resguardados fuera de la cadena (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; BID, 2020). La Figura 11 presenta un mapa regional de iniciativas por dominio, destacando los países y áreas de política pública donde se concentran los pilotos.

Figura 11

Mapa regional de iniciativas por dominio



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Según Allende López (2021a), LACChain, como programa catalizador, sistematizó un enfoque de redes permissionadas públicas con reglas operativas (roles de nodos, telemetría, criterios de operación y

auditorías periódicas) orientado a escalar desde pilotos hacia entornos de producción multiagencia. Su marco propone publicar metadatos y huellas criptográficas en la cadena —incluidas marcas de tiempo— y resguardar los documentos completos en repositorios con control de acceso, articulando interoperabilidad, privacidad y cumplimiento regulatorio.

Por su parte, el LACChain Identity Working Group (2021) desarrolla el LACChain ID Framework, que operacionaliza credenciales verificables, niveles de aseguramiento y lineamientos de custodia de claves para facilitar validaciones interorganismos sin exponer datos sensibles, junto con interoperabilidad entre billeteras y autoridades emisoras. La Tabla 12 detalla un inventario regional de pilotos y sus métricas principales.

Tabla 12
Inventario regional de pilotos y métricas

País	Plataforma	Diseño de datos	Métricas reportadas	Estado del proyecto	Inicio
Perú	LACChain	Metadatos y transacciones	Órdenes, proveedores, montos	Piloto realizado	2021
Colombia	Ethereum	Smart contracts	Órdenes, procesos, montos	En producción	2021
Chile	Hyperledger Fabric	Transacciones y trazabilidad	Interacción entre actores, montos	En análisis	2022
Argentina	Ethereum	Smart contracts	Órdenes, procesos, montos	En análisis	2022
Bahamas	No especificado	No especificado	No especificado	En producción	2020

Nota. Elaboración propia a partir de Foro Económico Mundial & Banco Interamericano de Desarrollo (2020) y Banco Interamericano de Desarrollo (2020).

2.4.2 Perú - PERÚ COMPRAS en LACChain (contrataciones)

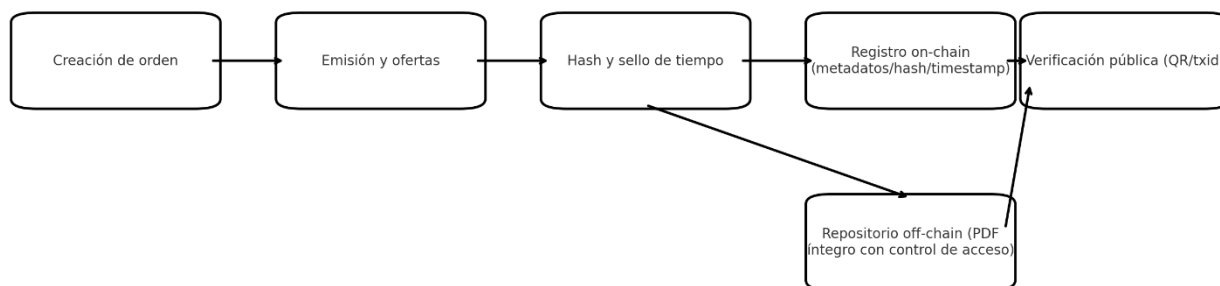
La experiencia de PERÚ COMPRAS es uno de los casos regionales más tempranos y medibles en compras públicas: desde 2019 registró órdenes de compra de sus Catálogos Electrónicos en una red tipo

LACChain, con el objetivo de reforzar trazabilidad documental y verificación pública. En septiembre de 2020 la entidad informó que “ha registrado en blockchain un total de 154,400 órdenes de compra”, lo que ilustra escala y continuidad del piloto (Gestión, 2020).

El diseño técnico separa deliberadamente on-chain y off-chain: la orden y sus ofertas quedan referenciadas mediante huellas criptográficas y sellos de tiempo, mientras el PDF íntegro se conserva en repositorios bajo control administrativo, accesible mediante verificación (PERÚ COMPRAS – CENTRAL DE COMPRAS PÚBLICAS, 2020). De este modo se ofrece prueba de no alteración sin exponer información sensible y se habilitan controles de auditoría sobre documentos completos cuando corresponde (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Figura 12 esquematiza el flujo técnico de publicación de órdenes.

Figura 12

Flujo técnico de publicación de órdenes de compra en PERÚ COMPRAS



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Perú Compras – Central de Compras Públicas (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

En términos de gobernanza, la institucionalización del caso se apoya en instrumentos internos como la Resolución Jefatural 139-2021, que aprueba la Directiva 006-2021, y en lineamientos de contratación electrónica previos; ese andamiaje normativo resulta clave para pasar de piloto a operación sostenida (Perú Compras – Central de Compras Públicas, 2021). A nivel regional, las guías del Foro Económico Mundial y el BID insisten en reglas explícitas de membresía, quórums y publicación responsable: la utilidad no proviene del “blockchain” per se, sino de cómo se gobiernan datos y responsabilidades a lo largo del ciclo de compra (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 13 resume parámetros de implementación del caso.

Tabla 13
Parámetros de implementación PERÚ COMPRAS

Parámetro	Campo/definición	Valor objetivo (piloto)	Evidencia/medición	Responsable
Campos mínimos on-chain	txid; hash del PDF; timestamp; estado; ID de orden; ID de pliego	Definir catálogo base	Consulta on-chain (API/CLI)	TI + Compras
Artefactos off-chain	PDF íntegro; pliego; ofertas; actas (con control de acceso)	Repositorio seguro operativo	Hash recalculado = hash publicado	Archivo + TI
Latencia objetivo de anclaje	Tiempo entre emisión/acto y publicación on-chain	≤ 15 min (p.ej.)	Métrica de ETL/cola + evento on-chain	TI
Roles y quórum para cambios	Membresía; despliegue de contratos; cambios críticos	$\geq 2/3$ validadores (ejemplo)	Acta firmada + registro on-chain	Gobernanza de red
Métricas operativas	% órdenes con hash verificable; discrepancias on/off-chain; tiempo de ciclo	$\geq 95\%$ verificable; $\leq 1\%$ discrepancia	Panel de métricas; auditorías	Compras + Auditoría

Nota. Elaboración propia a partir de Perú Compras – Central de Compras Públicas (2020); Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

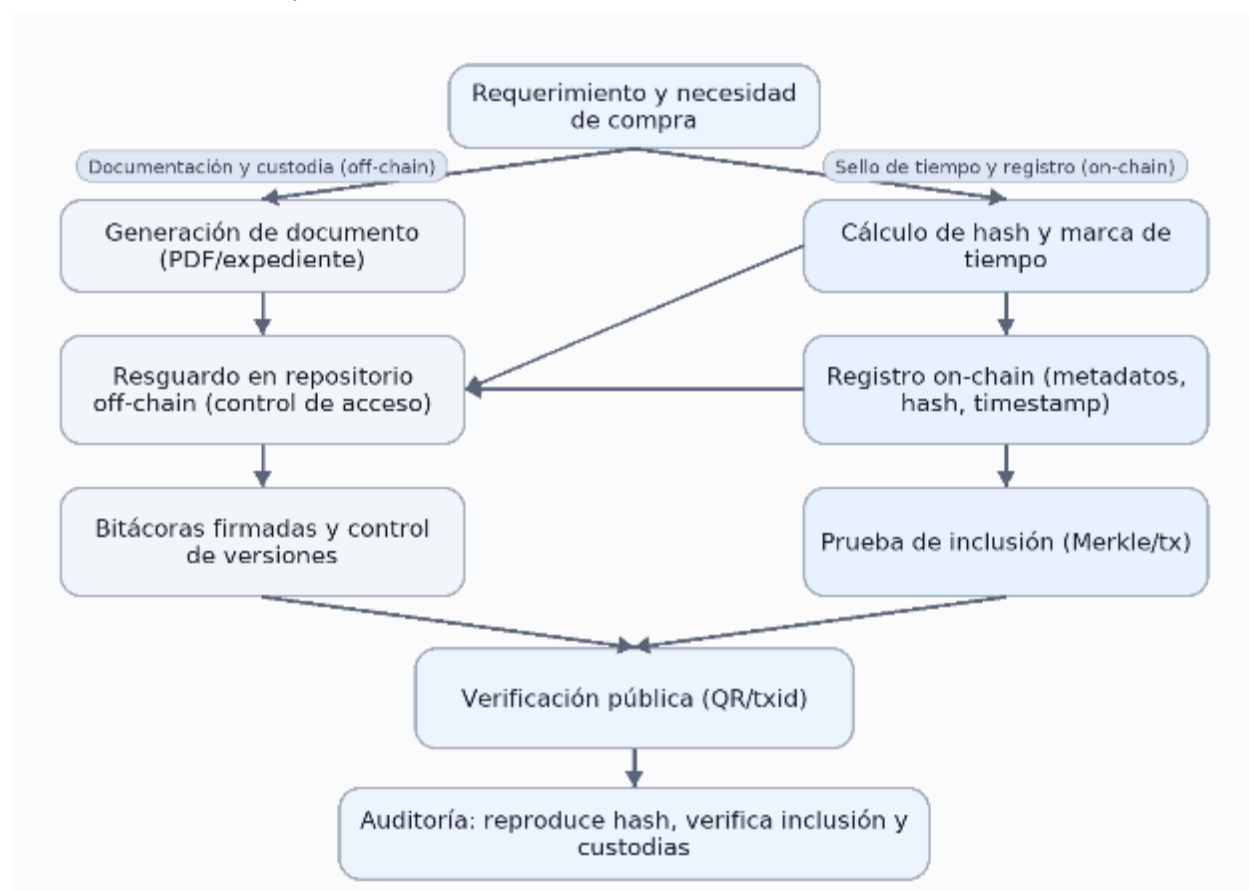
Operativamente, PERÚ COMPRAS indicó que cada orden se vincula con un código QR que permite acceder al documento original y comprobar su autenticidad, y que la información relevante se replica en varios nodos de la red, disminuyendo la probabilidad de alteraciones no detectadas (Perú Compras – Central de Compras Públicas, 2020). Esta capa de verificabilidad pública se alinea con el enfoque de LACChain de redes permissionadas con identidades fuertes y telemetría orientada a producción multiagencia (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

El caso confirma que las métricas relevantes exceden el conteo de órdenes: importan los tiempos de ciclo (requerimiento→adjudicación), la oportunidad de evidencia (latencia emisión→anclaje) y la

consistencia on/off-chain (hash verificable del PDF). La literatura recomienda incorporar estos indicadores desde el inicio del piloto y fijar umbrales de finalidad y publicación para reducir discrecionalidad (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Figura 13 integra estos elementos en un esquema de cadena de custodia verificable.

Figura 13

Cadena de custodia verificable



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Perú Compras – Central de Compras Públicas (2020) y Banco Interamericano de Desarrollo (2020).

2.4.3 Colombia - bono digital en blockchain (regulación/finalidad)

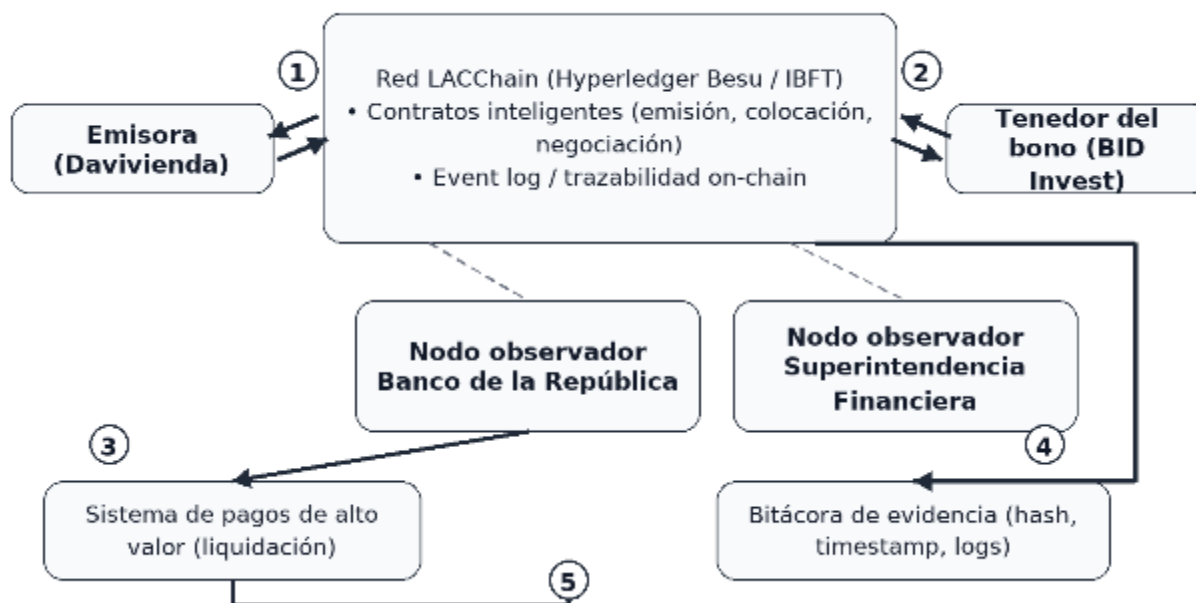
Colombia desarrolló un piloto regulatorio de bono completamente on chain —emisión, colocación, negociación y liquidación instrumentadas por contratos inteligentes sobre LACChain— en un entorno de prueba supervisado por la Superintendencia Financiera (Arenera), interoperando con el sistema de pagos de alto valor del banco central y apoyándose en una red permissionada con finalidad práctica (IBFT/QBFT)

(Inter-American Development Bank, 2022; Superintendencia Financiera de Colombia, 2022). Esta arquitectura permite medir tiempos de ciclo y asegurar finalidad de liquidación sin depender de finalidades probabilísticas de redes públicas, manteniendo trazabilidad y custodia de evidencia técnica (Banco de la República, 2023; Kaleido, 2019, 2023).

Según el banco central, el piloto de 2022 involucró un bono por 110 millones de pesos, con emisión, colocación y negociación en blockchain y liquidación cursada por el sistema de pagos de alto valor, con nodos observadores en el emisor y el supervisor, reduciendo incertidumbre operativa y documentando el rastro de extremo a extremo (Banco de la República, 2023). La Figura 14 representa la arquitectura del piloto.

Figura 14

Arquitectura del piloto: emisora y tenedor en LACChain



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco de la República (2023) e Inter-American Development Bank (2022).

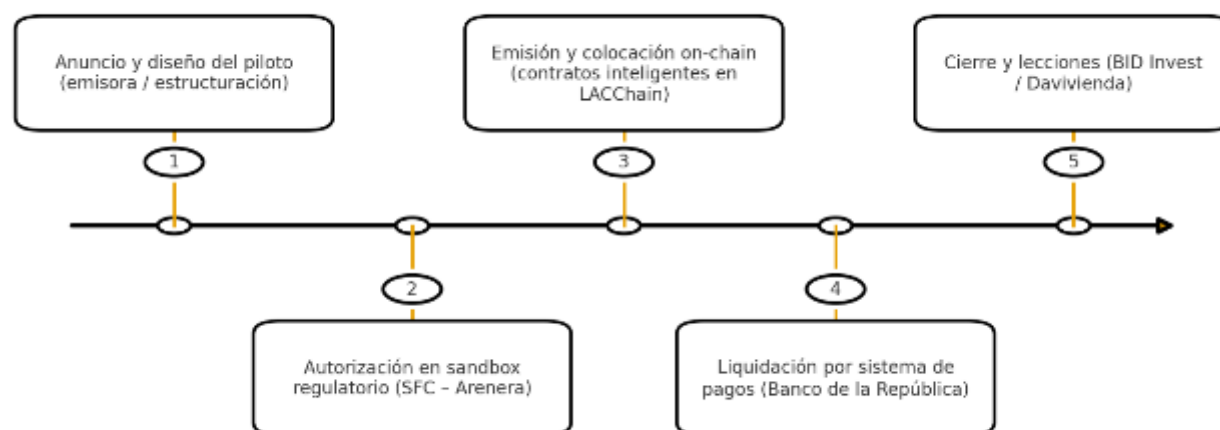
El Grupo BID sintetiza el alcance señalando que “el bono fue emitido, colocado, negociado y cumplido utilizando contratos inteligentes [...] y todas las operaciones se realizaron enteramente en blockchain” (Inter-American Development Bank, 2022). El objetivo fue verificar, a lo largo del ciclo de vida del título, posibles reducciones de costos operativos, optimización de tiempos, mayor trazabilidad y

seguridad, menor asimetría de información y mejor manejo de riesgos (Inter-American Development Bank, 2022; Banco de la República, 2023; Superintendencia Financiera de Colombia, 2022).

LACChain (Hyperledger Besu) opera con consenso BFT (IBFT/QBFT), que otorga finalidad determinista en segundos, atributo clave para títulos de renta fija y coordinación con ventanillas de pago y custodia (Kaleido, 2019, 2023). Este rasgo explica la elección de red permitida para un piloto regulado de mercado de capitales (Inter-American Development Bank, 2022).

En cuanto a habilitantes normativos, el piloto se enmarcó en el sandbox de la SFC (“Arenera”), que permite pruebas controladas con objetivos, métricas y salvaguardas definidos, bajo monitoreo del supervisor (Superintendencia Financiera de Colombia, 2022). Para este trabajo, ese encuadre sugiere una ruta de adopción: pruebas acotadas con validación de métricas y controles antes de escalar a operaciones regulares (Banco de la República, 2023; Inter-American Development Bank, 2022). La Figura 15 muestra la línea de tiempo del bono digital.

Figura 15
Línea de tiempo del bono digital



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Inter-American Development Bank (2022); Banco de la República (2023); Superintendencia Financiera de Colombia (2022).

El caso colombiano aporta tres lecciones: necesidad de finalidad práctica y baja latencia en red permitida; integración con la infraestructura crítica de pagos del banco central; y sandbox con métricas explícitas de eficiencia, trazabilidad y seguridad, bajo roles y salvaguardas regulatorias claras

2.4.4 Chile - CNE y notarización de datos (integridad/acceso)

La Comisión Nacional de Energía (CNE) incorporó blockchain en su portal de datos abiertos para certificar integridad y trazabilidad de información sectorial, convirtiéndose en 2018 en la primera entidad pública chilena en hacerlo. La decisión se inscribió en una política de innovación orientada a “aumentar los niveles de seguridad, integridad, trazabilidad y confianza” de la información publicada (Comisión Nacional de Energía [CNE], 2018b). Desde entonces, la certificación se ofrece a través de Energía Abierta y un validador público que permite verificar certificados emitidos para conjuntos de datos críticos del sector (Comisión Nacional de Energía, 2018a; Comisión Nacional de Energía, 2018b).

El diseño técnico separa evidencias criptográficas y contenido: on-chain se registran huellas (hash), marcas de tiempo y metadatos mínimos; off-chain se preservan los archivos íntegros (series y documentos) accesibles por API o descarga, alineando transparencia con protección de datos. En el lanzamiento, la CNE señaló la certificación de series como costos marginales promedio del Sistema Eléctrico Nacional, precios de combustibles y cumplimiento de la Ley de Energías Renovables, entre otros conjuntos que inciden en regulación y mercados (CNE, 2018a, 2018b). Bajo este esquema, un tercero puede recalcular el hash de un archivo y cotejarlo con el anclado en la cadena, reforzando confianza sin exponer información personal ni comercial sensible (Comisión Nacional de Energía, 2018a; Comisión Nacional de Energía, 2018b). La Figura 16 muestra el pipeline de certificación de la Comisión Nacional de Energía (CNE), desde la ingesta de datos hasta la publicación certificada y su verificación pública.

Figura 16
Pipeline de certificación CNE

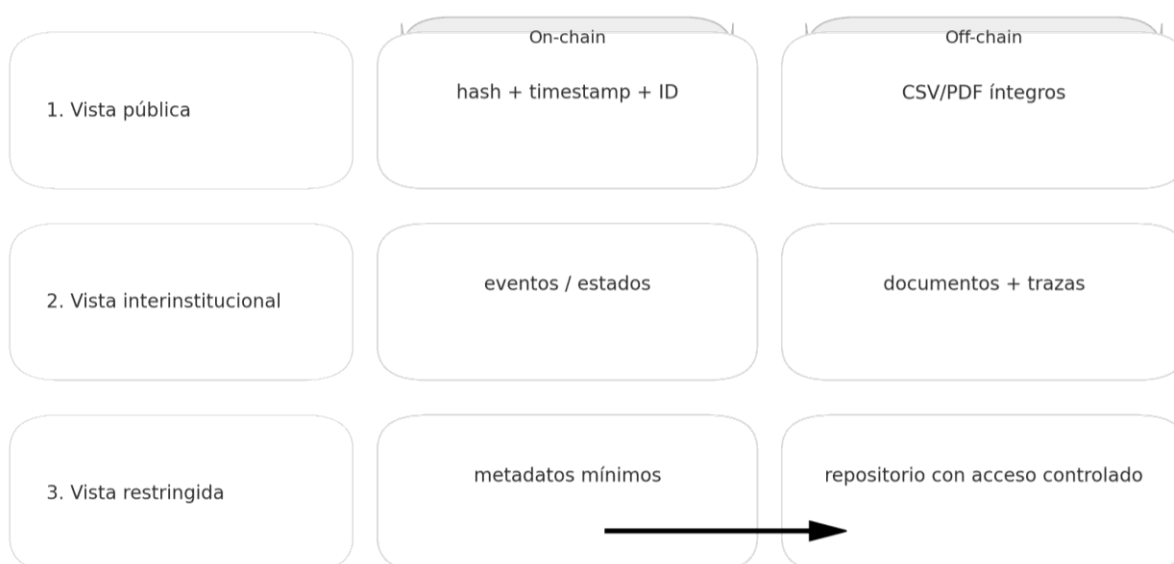


Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Comisión Nacional de Energía (2018a, 2018b).

En términos de acceso, el caso chileno dialoga con el principio de máxima divulgación y las excepciones legales: la Ley 20.285 consagra el derecho de acceso a la información pública, mientras la Ley 19.628 exige resguardar datos personales. Publicar metadatos verificables y huellas criptográficas satisface transparencia y, a la vez, limita la exposición de datos identificables, de modo que la verificación pública de integridad no implique revelar contenido protegido (Chile, 1999, 2008). La comunicación institucional destacó que la certificación ayuda a “elevar los estándares que certifican la calidad y certeza de los datos” disponibles para el ecosistema (CNE, 2018b).

Operativamente, el patrón CNE ofrece lecciones transferibles al dominio contable: gobernar catálogos y versiones, anclar hashes de archivos maestros y reportes, publicar metadatos con enlace de verificación y medir oportunidad de evidencia (latencia actualización→certificación), porcentaje de conjuntos con huella vigente y uso del validador. La Figura 17 sintetiza un modelo de acceso e integridad que combina publicaciones verificables, resguardo documental y límites legales de acceso.

Figura 17
Modelo de acceso e integridad



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Chile (1999, 2008) y Comisión Nacional de Energía (2018a, 2018b).

2.4.5 Argentina - QuarkID y BFA (identidad/consorcio)

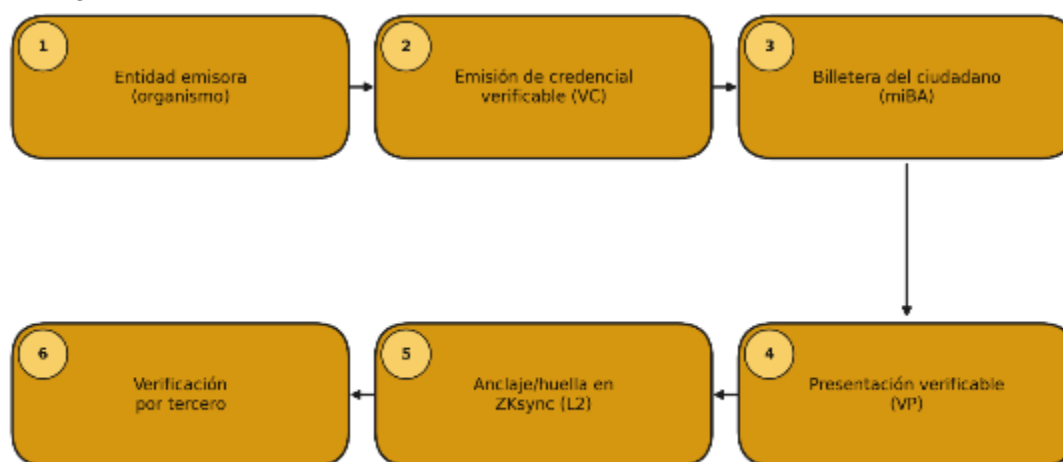
La trayectoria argentina combina una iniciativa de identidad digital con anclaje público —QuarkID, impulsada por la Ciudad de Buenos Aires— y una red permissionada de alcance federal —Blockchain Federal Argentina (BFA)— que desde 2017 ofrece notarización y trazabilidad para documentos y eventos.

En conjunto, ilustran dos patrones complementarios: credenciales verificables para personas (QuarkID) y una infraestructura de consorcio para registrar evidencias técnicas sin exponer datos sensibles (BFA) (Gobierno de la Ciudad de Buenos Aires, 2025; Blockchain Federal Argentina, s. f.).

En materia de identidad digital, la Ciudad de Buenos Aires integró QuarkID a miBA para permitir que distintos organismos emitan credenciales verificables cuya integridad se respalda en una cadena pública. Un comunicado oficial señala que “miBA incorporó la tecnología de QuarkID [...] con un respaldo de seguridad en la tecnología blockchain de ZKsync” (Gobierno de la Ciudad de Buenos Aires, 2025). Asimismo, la resolución que crea la plataforma QuarkID detalla sus servicios y componentes —incluida la interacción con la red ZKsync— y permite identificar con claridad los roles de emisión, custodia de claves y publicación de evidencias, sin exposición directa de datos personales (Gobierno de la Ciudad de Buenos Aires, 2024).

Este caso resulta relevante porque muestra una implementación concreta de credenciales verificables en el sector público argentino, donde la blockchain no sustituye los sistemas administrativos existentes, sino que actúa como capa de respaldo criptográfico y mecanismo de verificabilidad externa, aportando trazabilidad y fortaleciendo la confianza institucional. La Figura 18 representa la arquitectura general de QuarkID.

Figura 18
Arquitectura QuarkID



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Gobierno de la Ciudad de Buenos Aires (2024, 2025).

Desde el ángulo de infraestructura de consorcio, BFA se presenta como “red pública permitida” con validación por Prueba de Autoridad, orientada a que “cualquier organización implemente servicios [...]”

con garantías de inmutabilidad y trazabilidad sin necesidad de usar criptomonedas” (Blockchain Federal Argentina, s. f.). La red ofrece sellado de tiempo y registro de evidencias (hashes, marcas de tiempo) para certificar integridad de trámites y documentos, con enlaces públicos de verificación (por ejemplo, tsagui.bfa.ar) y guías para integrar el sellado en sistemas existentes (Blockchain Federal Argentina, s. f.).

QuarkID aporta un marco de credenciales verificables con anclaje público y control ciudadano sobre atributos; BFA, un riel de consorcio para evidencias técnicas en procesos administrativos (hashes de documentos, marcas de tiempo, bitácoras de eventos), útil para auditoría y archivo. En términos de medición, la combinación sugiere indicadores como tiempo emisión→verificación de credenciales, porcentaje de certificados con hash verificable en red pública, latencia de anclaje, tasa de discrepancias on/off-chain y cobertura de eventos auditables. A nivel de gobernanza, se requieren políticas de claves (HSM/MPC), RACI para emisores y verificadores y publicación responsable de metadatos, utilizando la red pública solo como prueba de integridad y no como repositorio de datos personales (Gobierno de la Ciudad de Buenos Aires, 2025; Blockchain Federal Argentina, s. f.). La Tabla 14 compara QuarkID y BFA.

Tabla 14
Comparación QuarkID–BFA

Etapas	QuarkID (proc·evid·ON/OFF)	BFA (proc·evid·ON/OFF)	Controles clave
Emisión	Emisión de VC · VC firmada+metadatos · OFF	Documento oficial · PDF firmado+metadatos · OFF	Firmas válidas; custodia de claves emisoras
Hash / anclaje	Anclaje L2 (ZKsync) · hash+ts+txid · ON	Hash+timestamp on-chain · hash+ts+txid · ON	Quóruns/red permisionada; gestión de claves
Almacenamiento	Wallet ciudadana+resguardo · DID/VC+ref anclaje · OFF	Repositorio off-chain · PDF íntegro+logs · OFF	Control de acceso; política de retención
Presentación / verificación	VP ante tercero · prueba vs anclaje · MIXTO	Portal/QR con recomputo · inclusión+txid · ON	Trazas de verificación; no repudio
Auditoría / monitoreo	Eventos/Revocación · logs/estados · ON	Monitoreo continuo · logs+actas/quórum · ON	Quóruns para cambios; auditorías periódicas

Nota. Elaboración propia a partir de Gobierno de la Ciudad de Buenos Aires (s. f., 2025) y Blockchain Federal Argentina (s. f.).

2.4.6 Síntesis y ruta de madurez

Los casos regionales más citados en compras públicas muestran mejoras en dos frentes: reducción de discrecionalidad percibida y trazabilidad de hitos. El ciclo típico documenta anclaje verificable de pliegos y versiones, registro de recepción de ofertas con sello de tiempo y publicación de adjudicaciones y pagos con referencias criptográficas. Siempre que se gobiernen membresías, quórums y publicación responsable, se observan mejoras en tiempos de ciclo y capacidad de auditoría (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). En identidad y certificaciones, los pilotos se concentran en diplomas, licencias o permisos con verificación pública del estado de un atributo (vigente/revocado), manteniendo el dato personal fuera de la cadena y exponiendo, en cambio, pruebas de integridad y eventos de revocación (LACChain Identity Working Group, 2021).

Un aprendizaje transversal es la utilidad del anclaje público para dotar de prueba independiente de no alteración a repositorios cerrados. Los diseños regionales más prudentes combinan redes permissionadas BFT de baja latencia y finalidad práctica con anclajes periódicos en una cadena pública, de modo que la auditoría interinstitucional se apoya en identidades fuertes y trazabilidad on-chain, y la auditoría social, cuando corresponde, verifica integridad por medio de hashes y marcas de tiempo accesibles sin exponer contenido sensible (BID, 2020; Allende López, 2021a). Esta separación técnica requiere procesos de datos consistentes: diccionarios versionados, políticas de minimización, linaje reproducible y bitácoras firmadas de transformaciones. La Figura 19 propone una ruta de madurez y escalamiento para proyectos de blockchain público, articulando etapas y carriles de trabajo en gobernanza, datos, operación y auditoría.

Figura 19
Ruta de madurez y escalamiento

	Piloto controlado	Beta regulatoria	Producción multiagencia
Gobernanza	Membresía inicial RACI y actas Umbral de voto	Quórum Change management Claves: HSM/multifirma	Estatuto del consorcio Incorporar/retirar miembros Auditorías periódicas
Datos/Privacidad	Diccionarios Minimización on-chain Hash + timestamp	Clasificación Vistas por audiencia Repositorio off-chain	ZK cuando aplique Retención Acceso por rol
Operación/Desempeño	Pruebas de carga SLOs Métricas básicas	Alta disponibilidad Alertas Telemetría de red	DRP/BCP Continuidad 24x7 Escalamiento por dominios
Auditoría	Evidencias mínimas Trazas de eventos Plan de pruebas	ISSAI 100 Muestreo/analytics Panel de riesgos	Auditorías programadas Métricas de efectividad Gestión de hallazgos

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Allende López (2021b) y LACChain Identity Working Group (2021).

Desde la perspectiva probatoria, la evidencia útil para auditoría se concibe como un conjunto de artefactos técnicos —hashes, sellos de tiempo, pruebas de inclusión, eventos de contratos— más la documentación de su obtención y custodia. En términos doctrinarios, el estándar aplicable se mantiene: el auditor debe obtener “evidencia suficiente y apropiada” para sustentar sus conclusiones, con atención a oportunidad y confiabilidad de las fuentes y a la posibilidad de que otro auditor competente comprenda los procedimientos y resultados (International Organization of Supreme Audit Institutions [INTOSAI], 2013, seccs. 43–45). Por ello, los diseños exitosos no se agotan en publicar transacciones, sino en demostrar la confiabilidad de los procesos que producen y resguardan tales evidencias.

En términos operativos, la literatura propone que la adopción de tecnologías de registro distribuido en contrataciones públicas y procesos administrativos avance sobre tres pilares: (a) reglas claras de membresía y quórum, con segregación de funciones y gestión de claves documentada; (b) modelos de

datos con publicación responsable y mecanismos de privacidad por diseño (separación on/off-chain, minimización de datos, control de acceso); y (c) métricas de desempeño y transparencia que permitan evaluar resultados (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Las entidades deben publicar metadatos verificables y evidencias criptográficas de integridad, evitando exponer información sensible, y sostener monitoreo continuo que documente decisiones y cambios relevantes en el ciclo del gasto.

La madurez observada en América Latina traza una secuencia repetible: pilotos controlados con métricas de eficiencia y transparencia; validación de gobernanza e identidad (membresía, quóruns, custodia de claves, credenciales verificables); y escalamiento por dominios con anclaje público. La agenda pendiente se ubica en el núcleo contable: llevar estos principios —publicación de metadatos, controles ex ante programables, auditoría continua— a asientos y conciliaciones presupuestarias, con indicadores de resultado (tiempos de auditoría, tasa de conciliaciones automáticas, verificabilidad de hashes y consistencia on/off-chain) que justifiquen la adopción a escala estatal (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Allende López, 2021b; LACChain Identity Working Group, 2021).

En América Latina existen guías y pilotos suficientes para pasar del concepto a implementaciones focalizadas. La continuidad de la agenda recae en procesos contables con métricas de resultado y validación probatoria, bajo consorcios permisionados con anclaje público y políticas de datos y claves que permitan sostener auditoría continua. Esta es la brecha que el diseño propuesto para el contexto argentino busca abordar.

2.5 Síntesis crítica y vacíos de investigación para Argentina

El estado del arte 2017–2025 muestra una convergencia programática y, a la vez, brechas operativas para el contexto argentino. En lo programático, la literatura ubica el núcleo de valor en (i) *triple entrada* como comprobante criptográfico compartido, (ii) *auditoría continua* sobre poblaciones completas y (iii) *separación responsable on/off-chain* para conciliar verificabilidad y confidencialidad (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019; Santos, 2022). En paralelo, los trabajos latinoamericanos más cercanos a la práctica enfatizan que los resultados dependen de gobernanza de consorcio, disciplina de datos y capacidades profesionales para traducir artefactos técnicos en evidencia aceptable (Morales, 2021; González González, 2023; Luna González Becerril, 2020; Yazuma Carrillo, 2023; Cambo Chillo, 2022). En términos de oficio, una tesis reciente recuerda que el profesional pasa a ser “participante clave en la fiabilidad de la información contable” (Polimandi, 2023, p. 1).

La literatura especializada sugiere que blockchain aporta cuando se integra a controles ex ante programables, metadatos públicos verificables y reglas de publicación; fuera de ese encuadre, la inmutabilidad consolida inconsistencias (Schmitz & Leoni, 2019; Foro Económico Mundial & Banco

Interamericano de Desarrollo, 2020). En América Latina, el optimismo técnico (mejoras de trazabilidad, eficiencia, reducción de asimetrías) convive con diagnósticos prudentes sobre costos de adopción, interoperabilidad y brechas de gobernanza (González González, 2023; Luna González Becerril, 2020). La conclusión comparada es operativa: el valor no proviene del on-chain per se, sino de cómo se gobiernan datos, roles y cambios, y de si la evidencia resultante es suficiente y apropiada para auditoría (Dai & Vasarhelyi, 2017; INTOSAI, 2013).

A la luz de este consenso, emergen cuatro brechas investigables y medibles:

Procesos contables de punta a punta (más allá de compras) con diseños cuasi-experimentales que midan *latencia documento→anclaje*, *% de asientos con hash verificable*, *discrepancias on/off-chain* y *tiempos de cierre* (Dai & Vasarhelyi, 2017; Morales, 2021).

Gobernanza y control interno: membresías, quóruns BFT y gestión de claves/identidades alineadas con COSO, con pruebas de efectividad de controles (COSO, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Validez probatoria: traducción de hashes, pruebas de inclusión y logs en *evidencia suficiente y apropiada*, documentando cadena de custodia y reproducibilidad (INTOSAI, 2013; Schmitz & Leoni, 2019; Cambo Chillo, 2022).

Capacidades profesionales: programas de formación que midan adquisición de competencias (lectura de eventos, re-hash, revisión de contratos) y su impacto en la calidad del aseguramiento (Santos, 2022; Polimandi, 2023).

Las guías internacionales recomiendan redes permissionadas con finalidad práctica y anclaje público de hashes, más publicación responsable (metadatos mínimos en cadena; documentos íntegros off-chain con control de acceso) (Banco Interamericano de Desarrollo, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). En contrataciones, la prospectiva regional secuencia estandarización de datos → automatización de controles → escalamiento con métricas, lo que es transferible a la contabilidad gubernamental si se fijan indicadores y criterios de éxito comparables (Yazuma Carrillo, 2023).

A los efectos de la auditoría del sector público, la ISSAI 100 mantiene como criterio central que la evidencia reunida sea suficiente (en cantidad y cobertura) y apropiada (en calidad, relevancia y confiabilidad), y que el trabajo quede documentado de manera que otro auditor competente pueda seguir los procedimientos aplicados y las conclusiones alcanzadas (INTOSAI, 2013, seccs. 43–45). En este trabajo, ese estándar se traduce en verificaciones criptográficas reproducibles (hash, timestamp y prueba de inclusión), conciliaciones on/off-chain, lectura de logs y revisión de controles embebidos, acompañadas de indicadores que miden latencia de publicación, discrepancias y cobertura de controles ex ante.

Agenda de investigación-acción propuesta.

Preguntas/Hipótesis. (a) ¿La publicación verificable reduce la latencia de evidencia y los tiempos de cierre? (b) ¿Los controles embebidos disminuyen discrepancias on/off-chain y retrabajos? (c) ¿La auditoría continua, con métricas explícitas, mejora la oportunidad y la suficiencia de la evidencia? (Dai & Vasarhelyi, 2017; Schmitz & Leoni, 2019).

Diseños. ITS (series temporales interrumpidas) para tiempos y latencias; DiD para comparar unidades piloto vs. control; cohortes para cobertura de controles y hallazgos repetidos (INTOSAI, 2013).

Indicadores. *P95 latencia documento→anclaje; % asientos con hash verificable; discrepancias por mil on/off-chain; tiempos de cierre; hallazgos repetidos; cobertura de controles ex ante* (Morales, 2021; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Condiciones de validez. Catálogos y esquemas versionados, RACI y quórums documentados, logs firmados, y pruebas reproducibles de hash/Merkle/eventos (COSO, 2013; INTOSAI, 2013; Cambo Chillo, 2022).

Situada en el punto de madurez del campo, la contribución de este trabajo será operacionalizar el consenso académico en un flujo contable auditable para Argentina: consorcio permissionado con finalidad rápida, anclaje público de metadatos y hashes, controles ex ante en contratos inteligentes, y panel de métricas alineado con ISSAI 100/COSO (Banco Interamericano de Desarrollo, 2020; COSO, 2013; INTOSAI, 2013). La originalidad reside en medir —no solo describir— el impacto en oportunidad de evidencia, consistencia on/off-chain y costo de verificación.

En síntesis, el estado del arte 2017–2025 muestra un consenso claro sobre el valor de la triple entrada, la auditoría continua y la separación on/off-chain, pero también evidencia brechas operativas para el caso argentino: calidad y gobierno de datos, gobernanza de consorcio, validez probatoria de las trazas técnicas y capacidades profesionales para traducirlas en evidencia suficiente y apropiada. Las líneas de investigación-acción propuestas organizan estas brechas en preguntas, diseños, indicadores y condiciones de validez que permiten pasar del discurso programático a intervenciones medibles en contabilidad gubernamental.

Sobre esta base, el Capítulo 3 profundiza en el marco institucional, normativo y ético que condiciona cualquier uso de blockchain en el sector público argentino. El objetivo es fijar con claridad los límites y obligaciones en materia de integridad, protección de datos, transparencia, prevención de la corrupción y acceso a la información, que luego orientarán tanto el diseño técnico de la solución como los criterios de evaluación empírica desarrollados en los capítulos siguientes.

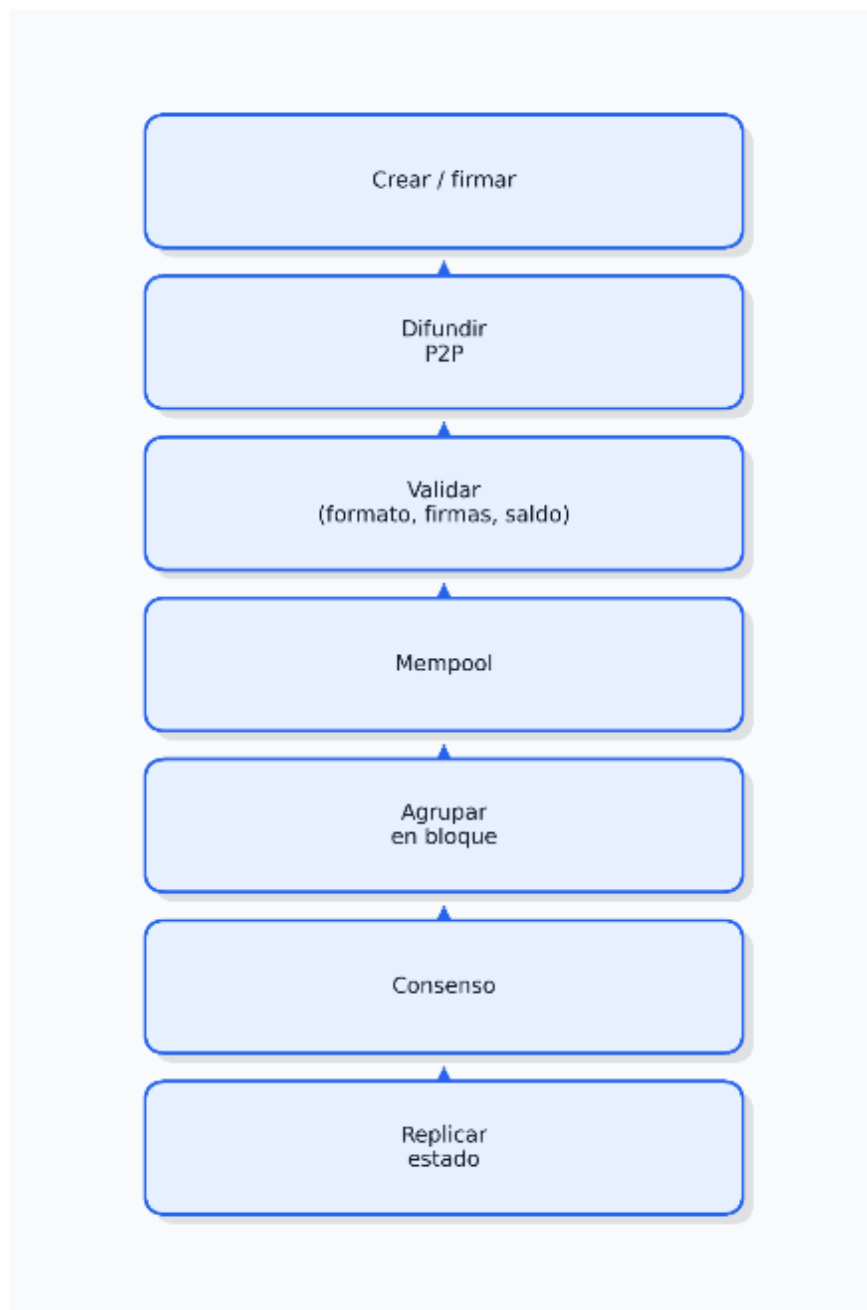
Capítulo 3: Marco teórico

3.1 Blockchain: concepto y fundamentos

Blockchain es una tecnología de registro distribuido (DLT) que mantiene un libro mayor compartido entre múltiples nodos y organiza la información en bloques encadenados mediante funciones hash. Cada bloque incluye un resumen criptográfico del bloque anterior, de modo que modificar un dato histórico implicaría alterar toda la cadena aceptada por la red, algo costoso de ejecutar y sencillo de detectar (Banco Interamericano de Desarrollo [BID], 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Morales, 2021; Santos, 2022). A diferencia de una base de datos centralizada, la confianza se apoya en reglas criptográficas y en un protocolo de consenso que coordina cómo se actualiza el libro mayor entre los participantes.

En términos fundacionales, la propuesta de Nakamoto (2008) introduce una red entre pares que permite resolver el problema del doble gasto sin depender de una entidad única de confianza. Esta idea inaugura un esquema en el que la validez de las transacciones se verifica colectivamente, y el registro resultante se comparte entre todos los nodos que participan en el consenso (Nakamoto, 2008). La Figura 20 presenta un esquema conceptual de blockchain, focalizado en los componentes necesarios para entender su aplicación en gestión pública.

Para efectos de este trabajo, se destacan tres propiedades particularmente relevantes para la gestión pública: (a) una inmutabilidad práctica del historial, derivada del encadenamiento de hashes y del uso de firmas digitales; (b) la posibilidad de reconstruir el recorrido completo de cada transacción (trazabilidad) desde su origen hasta su estado actual; y (c) la existencia de copias sincronizadas del registro en todos los nodos validadores (replicación consistente). En conjunto, estas características elevan el costo de cualquier alteración ex post, simplifican conciliaciones entre organismos y facilitan auditorías oportunas sobre información confiable (BID, 2020; Morales, 2021).

Figura 20*Esquema conceptual de blockchain*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Nakamoto (2008) y Banco Interamericano de Desarrollo (2020).

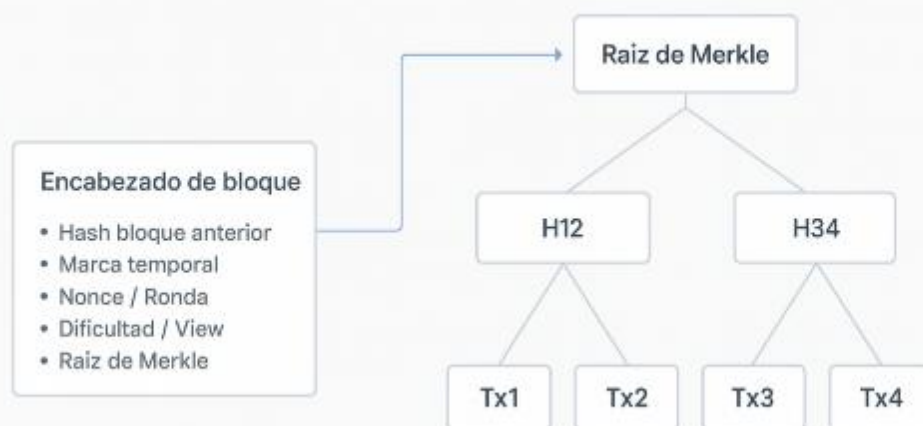
Las bases técnicas de blockchain se apoyan en desarrollos previos de criptografía aplicada. El uso de árboles de Merkle permite sintetizar grandes volúmenes de transacciones en una estructura que puede

verificarse con complejidad logarítmica; a su vez, los mecanismos de sellado temporal encadenado proporcionan evidencia de que el contenido no ha sido modificado a lo largo del tiempo. En una cadena de bloques, estas técnicas se combinan con el consenso distribuido para ofrecer un registro verificable y resistente a la manipulación (BID, 2020; Santos, 2022).

En plataformas de propósito general, la capa de contratos inteligentes agrega la posibilidad de programar reglas de negocio directamente sobre el libro mayor. Ethereum se describe como un libro de transacciones descentralizado que, además de almacenar estados, ejecuta código de manera determinista sobre ese estado compartido (Wood, 2014). Esto habilita la automatización de controles ex ante (por ejemplo, verificaciones presupuestarias o de límites de aprobación) y la generación de asientos acompañados de evidencia criptográfica común, cercana a la lógica de “triple entrada” que se discute en la literatura contable (Santos, 2022). La Figura 21 descompone las capas de una plataforma con contratos inteligentes, desde la infraestructura de red hasta las aplicaciones orientadas a procesos públicos.

Figura 21

Capas de una plataforma con contratos inteligentes



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Wood (2014); Santos (2022); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Desde la perspectiva del sector público, la forma en que se gobierna la red es tan importante como la tecnología subyacente. Las redes públicas maximizan apertura y verificabilidad ciudadana; las redes privadas concentran el control en una sola entidad; y las redes permissionadas o de consorcio distribuyen la

validación entre organizaciones identificadas, sujetas a reglas de membresía y responsabilidad (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; BID, 2020). En contextos gubernamentales se observa con frecuencia un patrón híbrido: una red permissionada que procesa datos sensibles y, en paralelo, un anclaje periódico de resúmenes criptográficos en una cadena pública para aportar prueba de integridad frente a terceros sin revelar el contenido de los registros (BID, 2020). La Tabla 15 compara una base de datos centralizada con una solución basada en blockchain aplicada a la gestión pública, resaltando implicancias para integridad, trazabilidad y auditoría.

Tabla 15

Comparación entre base de datos centralizada y blockchain en uso público

Propiedad	Definición operativa	Implicancias
Inmutabilidad	Encadenamiento de hashes y firmas que dificulta revertir asientos sin evidencia de alteración.	Reduce riesgos de manipulación ex post y facilita auditorías forenses.
Trazabilidad	Posibilidad de seguir el origen y recorrido de cada transacción en el libro mayor.	Mejora conciliaciones y permite reconstruir eventos con precisión temporal.
Replicación consistente	Todas las copias válidas convergen al mismo estado tras el consenso.	Asegura consistencia interinstitucional y minimiza discrepancias de cierre.
Contratos inteligentes	Código que ejecuta reglas y controles automáticos cuando se cumplen condiciones predefinidas.	Permite controles ex ante del gasto y segregación de funciones verificable.

Nota. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); Morales (2021).

En conjunto, el informe del Foro Económico Mundial y el Banco Interamericano de Desarrollo (2020) presenta a blockchain como una infraestructura capaz de reforzar integridad, trazabilidad y auditoría en el sector público de América Latina y el Caribe. El documento recomienda esquemas permissionados con anclaje en cadenas públicas para equilibrar confidencialidad y verificabilidad, y subraya que la adopción

efectiva requiere gobernanza interinstitucional clara, estándares de interoperabilidad, evaluación regulatoria y capacidades técnicas sostenibles.

3.2 Cómo funciona una red blockchain

El ciclo básico de una transacción en una red blockchain comienza con su creación y firma digital por parte del emisor. La firma vincula la operación con una clave privada y permite verificar autoría e integridad del mensaje. A continuación, la transacción se difunde en una red *peer-to-peer* para que los nodos la validen preliminarmente (formato, firmas, saldos o estados previos); mientras no se incluya en un bloque, permanece en una “mempool” accesible para los validadores (Nakamoto, 2008; Morales, 2021).

En la fase de construcción del bloque, los nodos que participan en el consenso agrupan transacciones en un bloque candidato. El encabezado del bloque contiene, entre otros datos, el hash del bloque anterior, una raíz de Merkle que resume el conjunto de transacciones y una marca de tiempo. Esta estructura implica que cualquier cambio en una transacción modifica la raíz de Merkle y, en cascada, los hashes de ese bloque y de todos los posteriores, lo que deja evidencia inmediata de alteración (BID, 2020; Morales, 2021). Cuando intervienen contratos inteligentes, se agregan metadatos de ejecución (por ejemplo, consumo de gas en plataformas compatibles con la Ethereum Virtual Machine), lo que facilita reconstruir la secuencia de eventos para fines de auditoría (Santos, 2022; Wood, 2014).

La incorporación definitiva del bloque depende del mecanismo de consenso. En redes públicas, la prueba de trabajo (PoW) asigna el rol de proponente al nodo que resuelve un problema criptográfico, lo que aporta seguridad a costa de un consumo energético elevado (Nakamoto, 2008). En prueba de participación (PoS), los validadores se seleccionan según su participación económica (*stake*) y reglas de penalización, logrando menor consumo y una finalidad más rápida. En entornos gubernamentales, las redes permissionadas suelen utilizar mecanismos tolerantes a fallos bizantinos (por ejemplo, PBFT o IBFT), donde los validadores son entidades conocidas y se alcanza una decisión determinística en segundos, con trazabilidad de responsabilidades por nodo (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 16 presenta una comparación sintética de los mecanismos de consenso más utilizados en redes públicas y permissionadas, con foco en seguridad, energía, finalidad y latencia.

Tabla 16*Comparativa de mecanismos de consenso para redes públicas y permissionadas*

Consenso	Seguridad	Energía	Finalidad	Latencia	Uso típico
PoW	Alta; ataque costoso	Muy alta	Probabilística (N bloques)	Minutos	Públicas muy descentralizadas
PoS	Alta; basada en stake/penalizaciones	Baja–media	Rápida/probabilística	Segundos–decenas de segundos	Públicas modernas y consorcios
BFT (PBFT/IBFT)	Alta con quórum conocido	Baja	Determinística (casi inmediata)	Sub-segundos–pocos segundos	Permissionadas con miembros identificados

Nota. Elaboración propia a partir de Nakamoto (2008); Wood (2014); Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Antes de aceptar un bloque, cada nodo verifica al menos tres aspectos: (i) la validez de firmas y la ausencia de doble gasto; (ii) la coherencia de los hashes del encabezado y del árbol de Merkle; y (iii) el cumplimiento de las reglas del protocolo, incluidos los límites de gas o cuotas en entornos con contratos inteligentes. Una vez alcanzado el consenso, los nodos añaden el bloque a su copia local y actualizan su estado, replicando el nuevo historial a toda la red (Morales, 2021; Santos, 2022).

En arquitecturas híbridas, este flujo se extiende con una etapa adicional de anclaje: se calcula un hash representativo del estado o de un lote de registros de la red permissionada, y ese hash se publica en una cadena pública. De este modo, se obtiene evidencia pública de integridad sin exponer el detalle de los datos subyacentes (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La secuencia crear y firmar → difundir → validar y empaquetar → consensuar → replicar genera un historial compartido, ordenado y verificable, adecuado para procesos contables que requieren evidencia técnica de integridad y de cierre de los asientos (BID, 2020; Morales, 2021; Santos, 2022). La integración de contratos inteligentes en este ciclo permite incorporar controles ex ante (validaciones presupuestarias, segregación de funciones, umbrales de aprobación) y facilitar conciliaciones ex post sobre la base de eventos registrados en la cadena.

En redes de consorcio, la identidad verificable de los validadores añade una capa de rendición de cuentas, mientras que el anclaje público ofrece una prueba independiente de no alteración frente a terceros.

La privacidad se gestiona mediante particiones lógicas (canales), cifrado de campos y, en casos avanzados, pruebas de conocimiento cero, de forma que la integridad pueda comprobarse sin revelar el contenido. Estas propiedades contribuyen a acortar tiempos de auditoría, mejorar la calidad de la evidencia y reducir el espacio para la discrecionalidad operativa (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Santos, 2022).

Sintetizando, distintas fuentes coinciden en que el valor de blockchain para la gestión pública reside menos en “escribir bloques” y más en la capacidad de coordinar confianza entre actores mediante reglas criptográficas, consenso y trazabilidad reproducible (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Morales, 2021; Santos, 2022).

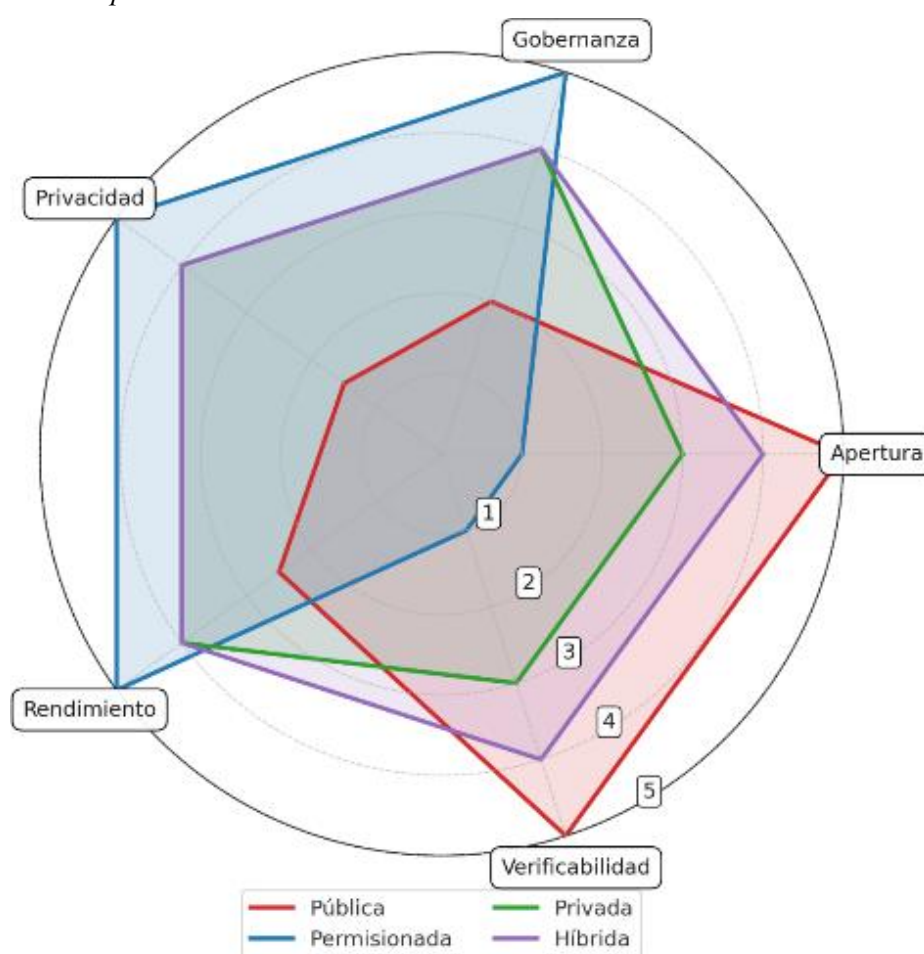
3.3 Tipos de blockchain

3.3.1 Introducción

Con fines de análisis y de diseño institucional, las implementaciones de cadena de bloques suelen agruparse en cuatro familias: redes públicas (*permissionless*), redes privadas, redes permissionadas de consorcio y arquitecturas híbridas (ver Figura 22). Cada una equilibra de manera distinta apertura, gobernanza, protección de datos, rendimiento y capacidad de verificación externa (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Figura 22

Mapa conceptual de tipos



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

3.3.2 Redes públicas (permissionless)

En las redes públicas, cualquier persona puede leer el libro mayor y, cumpliendo las reglas del protocolo, participar en la validación de bloques (por ejemplo, Bitcoin o Ethereum). La seguridad descansa principalmente en incentivos económicos y en mecanismos de consenso como PoW o PoS, que penalizan el comportamiento malicioso y encarecen los ataques (BID, 2020; Wood, 2014). Desde el planteo original de Nakamoto (2008), la moneda electrónica se concibe como una cadena de firmas digitales verificables sin intervención de una entidad financiera central, lo que habilita pagos entre pares con menor dependencia de intermediarios.

Estas propiedades potencian la transparencia y la verificabilidad abierta, pero también introducen desafíos para usos administrativos: la latencia y los costos de operación pueden resultar variables e incompatibles con ciertos plazos de gestión, y la privacidad es limitada por la naturaleza pública del libro mayor, aunque se use seudonimato (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). En términos generales, las cadenas públicas maximizan la descentralización y la auditoría ciudadana, a costa de un menor control institucional directo y de una exposición elevada de metadatos transaccionales (BID, 2020).

3.3.3 Redes privadas

Las redes privadas son administradas por una sola organización, que define quién puede operar nodos, acceder a los datos y participar en el consenso. Esto permite alcanzar altos niveles de rendimiento y simplificar la gobernanza, pero concentra la confianza en un único administrador y reduce significativamente las posibilidades de auditoría independiente (BID, 2020). En el ámbito contable estatal, pueden funcionar como bitácoras internas o capas de integridad sobre sistemas legados, siempre que se definan controles adecuados; sin embargo, su aporte a la transparencia pública es limitado si no se acompaña de algún mecanismo verificable por terceros que acredite la no alteración del historial (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

3.3.4 Redes permissionadas (de consorcio)

Las redes permissionadas de consorcio agrupan a varias entidades identificadas (por ejemplo, órganos de control, ministerios, empresas públicas) que comparten la validación bajo reglas explícitas de membresía, acceso y quórum. En este tipo de redes suele emplearse consenso BFT (como PBFT o IBFT), que brinda finalidad práctica en segundos y permite atribuir cada validación a nodos concretos, lo que refuerza la trazabilidad de responsabilidades (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). El Foro Económico Mundial y el BID (2020) señalan que estas

configuraciones permiten acordar un único historial entre actores conocidos, manteniendo controles finos sobre qué datos ve cada participante.

Para la administración pública, las redes de consorcio ofrecen un equilibrio entre rendimiento, cumplimiento normativo y auditoría interorganismos. No reproducen el grado de apertura de una cadena pública, pero facilitan la cooperación entre entidades del Estado y soportan esquemas de control compartido (BID, 2020). La Tabla 17 compara los tipos de red por dimensiones clave —apertura, gobernanza, privacidad, rendimiento y verificabilidad externa— con ejemplos orientativos de uso.

Tabla 17
Comparativa por dimensiones

Tipo	Apertura	Gobernanza	Privacidad	Rend./Lat.	Verif. externa	Ejemplos	Casos de uso
Pública	Alta	Protocolo e incentivos	Baja / seudónima	Variable (menor)	Máxima	Bitcoin; Ethereum	Auditoría abierta; notariado
Privada	Baja	Entidad única	Alta (accesos internos)	Alta	Limitada	Libro interno	Bitácoras; integridad de logs
Permisio nada	Media (miembros)	Consorcio	Alta (canales/particiones)	Alta (BFT)	Media–alta	Hyperledger Besu/Quorum; IBFT	Interagenci as; contratos; compras
Híbrida	Media (mixta)	Consorcio + anclaje	Alta (privado + hash)	Alta privado + costo anclaje	Alta (integridad pública)	Permisio nada + Ethereum (hashes)	Trazabilida d privada; certificació n de integridad

Nota. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

3.3.5 Arquitecturas híbridas

Las arquitecturas híbridas combinan una red privada o permissionada —donde se procesan los datos sensibles— con un anclaje periódico de resúmenes criptográficos en una cadena pública. El objetivo es obtener, a la vez, control institucional sobre la información y prueba pública de integridad. En este esquema,

los asientos, documentos y metadatos completos permanecen bajo custodia de las entidades autorizadas, mientras que la publicación de hashes en una red pública funciona como evidencia de no alteración frente a terceros (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Para registros contables gubernamentales, este patrón resulta especialmente adecuado: permite respetar restricciones de confidencialidad y protección de datos personales, a la vez que habilita mecanismos de verificación externa sobre la consistencia del historial. De este modo, se refuerza la rendición de cuentas sin sustituir los marcos legales existentes ni exponer información operativa crítica (BID, 2020). La Figura 23 ilustra el esquema de anclaje híbrido, en el que una red permissionada procesa datos sensibles y publica hashes en una cadena pública como prueba de integridad.

Figura 23

Esquema de anclaje híbrido



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020).

3.3.6 Criterios de elección

La literatura aplicada propone evaluar, antes de seleccionar un tipo de red, al menos seis dimensiones: (i) sensibilidad de los datos a tratar; (ii) necesidad de verificación externa o control social;

(iii) número y tipo de actores involucrados y el modelo de gobernanza previsto; (iv) requisitos de rendimiento y latencia; (v) presupuesto disponible y capacidades técnicas; y (vi) estrategia de escalabilidad y mantenimiento (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Morales, 2021; Santos, 2022). En el caso de las redes públicas, Nakamoto (2008) pone el énfasis en eliminar la dependencia de intermediarios financieros para permitir pagos entre pares; en contextos estatales, el foco se desplaza hacia integridad del registro, cumplimiento normativo y gobernanza multi-actor. La Tabla 18 organiza una matriz de decisión para seleccionar el tipo de red según sensibilidad de datos, necesidad de verificación externa, actores involucrados, rendimiento y capacidades operativas.

Tabla 18
Matriz de decisión

Criterio	Recomendación preferida	Justificación breve
Sensibilidad de datos	Permisiónada/Privada con anclaje	Control de acceso y canales/particiones
Necesidad de verificación externa	Híbrida (anclaje público) o Pública	Prueba pública de integridad sin exponer datos
Número de actores y gobernanza	Permisiónada (consorcio)	Reglas de membresía y atribución por entidad
Rendimiento y finalidad	Permisiónada (BFT)	Finalidad rápida para controles ex ante
Presupuesto y capacidades	Permisiónada o Híbrida	Operación coordinada de nodos y costos previsibles
Escalabilidad y segmentación	Permisiónada con canales + anclaje	Crecimiento sin comprometer confidencialidad

Nota. Criterios orientativos; la selección final debe alinearse con requisitos legales y capacidades operativas. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

A la luz de estos criterios, para procesos de registro y seguimiento de la ejecución presupuestaria se sugiere, como línea base, un consorcio permisionado (por ejemplo, OA, AGN, SIGEN y Hacienda) con anclaje público de hashes de bloque. Esta configuración permite programar controles ex ante mediante contratos inteligentes, alcanzar finalidad rápida para cierres contables y disponer de evidencia pública de integridad sobre los registros (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Santos, 2022). En términos sintéticos, las redes públicas aportan transparencia amplia; las privadas

concentran control operativo; las permissionadas permiten gobernanza compartida con buen desempeño; y el enfoque híbrido tiende un puente entre integridad verificable y confidencialidad institucional (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Morales, 2021; Santos, 2022; Wood, 2014). La Figura 24 sintetiza el modelo propuesto para la OA, combinando red permissionada de consorcio y anclaje público de hashes de bloque para los procesos contables priorizados.

Figura 24

Modelo propuesto para la OA



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

3.4 Beneficios para la gestión pública

La tecnología blockchain aporta beneficios concretos para la gestión pública cuando se alinea su diseño con objetivos institucionales: aumentar la transparencia de los registros, fortalecer la trazabilidad de operaciones, mejorar la integridad de la información contable y reducir tiempos y costos de auditoría (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Morales, 2021). En términos de gobernanza de datos, el libro distribuido permitir que múltiples organismos compartan un “único registro fuente” verificable, disminuyendo discrepancias y conciliaciones manuales, y habilitando auditorías continuas sobre evidencia criptográfica (BID, 2020).

Nakamoto (2008) subrayó el principio técnico que sustenta estos beneficios al afirmar: “Proponemos un sistema para transacciones electrónicas sin depender de la confianza” (p. 7). Esta

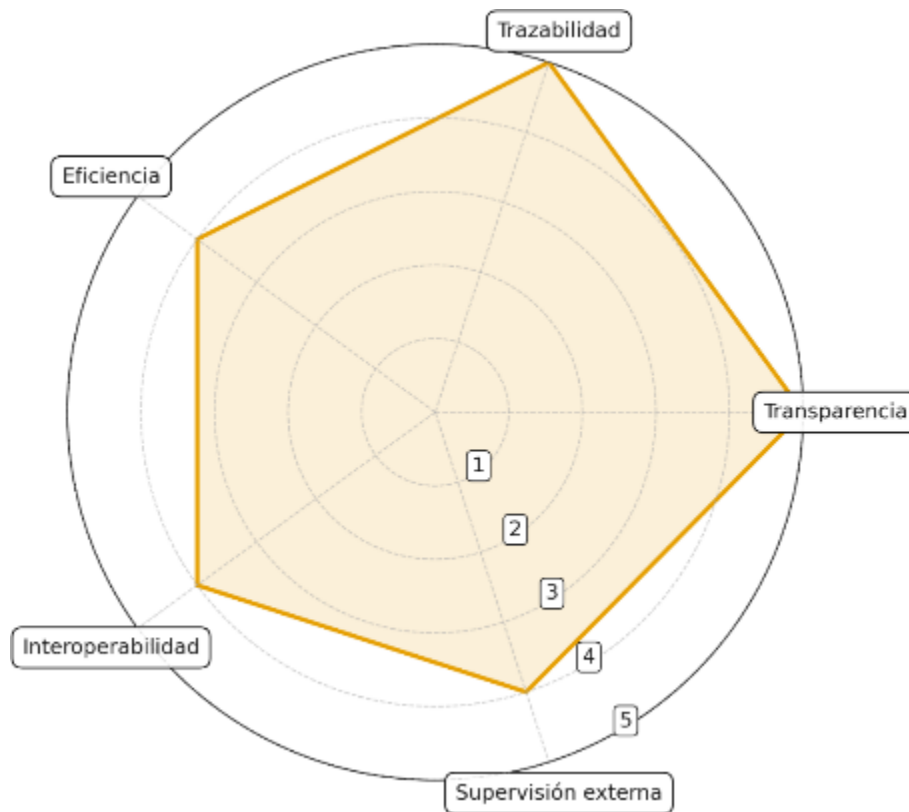
sustitución de confianza interpersonal por pruebas criptográficas se traducir, en contexto estatal, en controles ex ante programables y verificaciones independientes ex post. Asimismo, la llegada de plataformas de contratos inteligentes posibilitar “un libro de transacciones generalizado, seguro y descentralizado” (Wood, 2014, p. 1, “Introduction”), lo que extiende la trazabilidad a reglas y procesos automatizados (Santos, 2022).

Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, que permita a dos partes interesadas realizar transacciones directamente [...] La red marca las transacciones con una marca de tiempo mediante un algoritmo hash en una cadena continua de prueba de trabajo basada en hash, formando un registro que no se puede cambiar sin rehacer la prueba de trabajo. (Nakamoto, 2008, secc. “Abstract”).

La Figura 25 presenta un mapa de beneficios por dimensión —transparencia, trazabilidad, eficiencia, interoperabilidad y supervisión externa— aplicados a la gestión pública.

En materia de eficiencia operativa, la replicación consistente del registro contable y la inmutabilidad de los asientos disminuir la necesidad de conciliaciones y revisiones redundantes, con impacto directo en el costo de auditoría y en los tiempos de cierre (Morales, 2021). En licitaciones y contrataciones, los repositorios de bases y ofertas con sellos de tiempo verificables reducir la discrecionalidad y el riesgo de manipulación documental, a la vez que facilitan la supervisión interinstitucional (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). De forma complementaria, los contratos inteligentes permitir incorporar reglas de control “antes de pagar”: validación de crédito presupuestario, segregación de funciones, y umbrales de autorización, generando evidencia automática de cumplimiento en cada paso (Santos, 2022).

Desde la perspectiva de transparencia y rendición de cuentas, los mecanismos de publicación verificable —incluido el anclaje criptográfico en cadenas públicas— habilitar a auditores y terceros a comprobar que un conjunto de registros no fue alterado, sin exponer contenido sensible (BID, 2020). En ese sentido, la trazabilidad integral de expedientes y movimientos presupuestarios contribuir a mejorar la calidad del dato disponible para organismos de control y para la ciudadanía, lo que se traducir en mayor confiabilidad de los informes y tableros abiertos (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 19 sintetiza los beneficios esperados por proceso y organismo, tomando como referencia las experiencias y lineamientos internacionales.

Figura 25*Mapa de beneficios por dimensión*

Nota. Mapa de beneficios por dimensión (transparencia, trazabilidad, eficiencia, interoperabilidad, supervisión externa). Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

En clave de interoperabilidad, un libro mayor compartido entre OA, AGN, SIGEN y Hacienda ofrecer un soporte común para estados y movimientos, disminuyendo “islas” de información y errores de carga; además, la referencia por hash a documentos resguardados en repositorios seguros simplificar la localización de evidencia y su validación cruzada (BID, 2020). Cuando se combinan estos atributos con esquemas de gobernanza de red claros (membresía, permisos, auditoría de nodos), el resultado es una infraestructura con mejor resiliencia operativa y menor superficie para alteraciones no autorizadas (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Figura 26 presenta la teoría de cambio del proyecto, articulando insumos, actividades, resultados intermedios e impactos esperados en la gestión pública.

Tabla 19
Beneficios por proceso y organismo

Proceso	Intervenciones (OA/AGN/SIGEN/Hac.)	Beneficio	Evidencia
Presupuesto y compromiso	OA: crédito+trazas; AGN: control; SIGEN: SOD/flujo; Hac.: contab.+indic.	↓ conciliaciones; control automático.	Hash asientos/doc.; ts.
Devengado y pago	OA: liberación cond.; AGN: devengado vs doc.; SIGEN: alertas/umbral; Hac.: tesorería/conc. auto.	↓ reprocesos y reclamos.	Eventos on-chain; logs; hash comp.
Contrataciones	OA: hitos/actas públicas; AGN: cambios/adjud.; SIGEN: trazab. comité; Hac.: portales (SICOP/SIB/SIPE).	↓ discrecionalidad percibida.	Hash versiones; ts público.
Cierres y auditoría	OA: estados compart.; AGN: muestras por riesgo; SIGEN: cross-check; Hac.: consolidación/reportes.	Cierres rápidos; evidencia sólida.	Merkle e inclusión.

Nota. Beneficios estimados por proceso y organismo; su materialización depende del diseño de contratos y de la gobernanza de la red. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Figura 26
Teoría de cambio del proyecto



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Foro Económico Mundial & Banco Interamericano de Desarrollo (2020) y Morales (2021).

Con todo, los beneficios dependen de decisiones de diseño y política tecnológica: la red y sus contratos deben integrarse a procesos existentes, respetar marcos normativos y asegurar privacidad mediante particiones de datos, canales y técnicas criptográficas (BID, 2020; Santos, 2022). Un despliegue gradual —piloto, escalamiento por módulos y publicación progresiva de indicadores— mitigar riesgos y facilitar la adopción institucional (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 20 propone un conjunto de indicadores de beneficio para medir eficiencia, trazabilidad y transparencia a lo largo del ciclo de implementación.

Tabla 20
Indicadores propuestos de beneficio

Indicador	Definición	Línea de base	Meta piloto	Fuente/medición
Tiempo medio de conciliación	Horas entre cierre y conciliación final	Establecer con histórico de 12 meses	Reducir $\geq 30\%$ en piloto	Registros contables y bitácora de conciliación
Hallazgos repetidos (AGN/SIGEN)	Proporción de hallazgos repetidos sobre total	Establecer con histórico de 3 años	Reducir $\geq 25\%$	Informes de auditoría y red de evidencia
Diferencia de saldos entre sistemas	Incidencias por desvíos entre libros y tesorería	Línea base trimestral vigente	Reducir $\geq 40\%$	Tableros y reportes de conciliación
% operaciones con control ex ante	Operaciones con validación automática sobre total	Medir en mes 1 del piloto	Alcanzar $\geq 85\%$	Logs de contratos y métricas de red
Tiempo de respuesta a requerimientos	Días hasta entregar evidencia solicitada	Promedio anual anterior	Reducir $\geq 35\%$	Mesa de entradas + hash de expedientes

Nota. Métricas orientativas; la línea de base debe fijarse con datos históricos del organismo. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020) y Morales (2021).

La literatura converge en que blockchain aportar valor público cuando se orienta a problemas específicos de integridad e interoperabilidad: (a) disminuir costos de verificación y tiempos de auditoría, (b) fortalecer la trazabilidad y la transparencia verificable, y (c) habilitar controles automatizados que

reduzcan la discrecionalidad en el ciclo del gasto (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Morales, 2021; Santos, 2022).

3.5 Desafíos contables en el Estado

3.5.1 Introducción

La adopción de blockchain en procesos contables públicos concentra desafíos técnicos, normativos, organizacionales y de gestión de datos que condicionan su viabilidad e impacto. El Banco Interamericano de Desarrollo subraya que el éxito no radica solamente en la herramienta, sino en “cómo se gobiernan los datos, qué actores participan y bajo qué reglas de intercambio y auditoría” (Banco Interamericano de Desarrollo [BID], 2020, secc. Gobernanza de datos) y en que los proyectos se alineen con “objetivos públicos verificables y medibles” (BID, 2020, secc. Criterios de selección).

En términos operativos, diversos autores coinciden en que la arquitectura institucional y la calidad de los datos pesan tanto como el tipo de cadena o el algoritmo de consenso. Por ello, la decisión tecnológica debe venir después de explicitar quién valida, cómo se resuelven conflictos, qué evidencias quedan disponibles para auditoría y cómo se resguardan los datos sensibles (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). A su vez, marcos consolidados de control interno, como COSO, recuerdan que el ambiente de control, la evaluación de riesgos, las actividades de control, la información y comunicación, y el monitoreo deben diseñarse de forma coherente con los objetivos de reporte y cumplimiento (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013). Desde la auditoría del sector público, ISSAI 100 exige evidencia suficiente y apropiada, criterios claros y responsabilidades definidas, lo que obliga a traducir la “inmutabilidad” técnica en trazabilidad institucional y procesos auditables (International Organization of Supreme Audit Institutions [INTOSAI], 2013).

Implementar blockchain en el sector público requiere una gobernanza explícita del consorcio, reglas de membresía, responsabilidades trazables y un diseño documental que preserve la integridad sin vulnerar la confidencialidad. La tecnología es condición necesaria, pero no suficiente: el valor público proviene de las reglas y de su cumplimiento efectivo (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, secc. Recomendaciones). El problema a resolver es de coordinación y calidad de información: sin datos normalizados, roles claros y controles verificables, una cadena de bloques no corrige las deficiencias de origen (BID, 2020).

Cuando, en cambio, existen múltiples partes que no confían plenamente entre sí, se requiere auditoría casi en tiempo real y es posible establecer reglas comunes de operación, la tecnología adquiere sentido práctico (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Figura 27 organiza en una taxonomía los principales desafíos de la adopción de blockchain en contabilidad pública,

diferenciando aspectos técnicos, organizacionales, normativos y de capacidades.

Figura 27

Taxonomía de desafíos blockchain en contabilidad pública



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

La viabilidad de blockchain en contabilidad pública depende de alinear diseño institucional, gobierno de datos y objetivos de control. Sin ese encuadre —desde COSO e ISSAI 100 hasta las guías específicas para sector público—, la “programabilidad” y la “inmutabilidad” quedan subutilizadas o generan nuevos riesgos (BID, 2020; COSO, 2013; INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 21 sintetiza los riesgos identificados y las líneas de mitigación asociadas, enmarcadas en los estándares de control interno y auditoría del sector público.

Tabla 21
Síntesis de riesgos y líneas de mitigación

Dimensión	Riesgo típico	Consecuencia	Mitigación sugerida
Técnicos	Elección inadecuada de consenso/red	Baja finalidad o caídas de rendimiento	Red permitida BFT para cierres; pruebas de carga; SLOs
Datos	Catálogos/formatos heterogéneos	Asientos no conciliables on-chain	ETL con validaciones; diccionario de datos; versionado
Gobernanza	Roles y quórum difusos	Bloqueos o cambios discrecionales	Acuerdo de consorcio; RACI; políticas de membresía
Privacidad	Sobreexposición de metadatos	Riesgo legal/reputacional	Separación on/off-chain; ZKP; canales privados
Rendimiento/finalidad	Latencia alta, reversiones	Cierres contables inciertos	Consenso con finalidad rápida; ventanas de cierre
Auditoría/evidencia	Pruebas no adaptadas a on-chain	Hallazgos débiles	Mapear ISSAI 100 a artefactos (hash, Merkle, logs)
Integración con legados	ETL sin controles	Duplicación/pérdida de documentos	APIs firmadas; trazabilidad de lotes; checksum de anexos
Identidades y llaves	Pérdida/uso indebido de claves	Asientos inválidos	HSM/MPC; rotación y revocación; 2FA para firmas
Costos y capacidades	Falta de perfiles mixtos	Subutilización de la red	Plan de capacitación; operación 24x7; monitoreo
Marco legal y responsabilidad	Evidencia no reconocida	Impugnación de registros	Políticas de sello de tiempo/hash; normativa aplicable

Nota. Las medidas deben alinearse con objetivos de control, requisitos legales y capacidades operativas de los organismos participantes. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020), Foro Económico Mundial & Banco Interamericano de Desarrollo (2020), COSO (2013) e INTOSAI (2013).

3.5.2 Calidad, normalización e interoperabilidad de datos

La base de cualquier contabilidad distribuida en el Estado es la calidad del dato. Cuando los asientos provienen de múltiples aplicaciones, formatos y criterios de clasificación, el resultado típico es un mosaico difícil de conciliar. En este escenario, registrar “tal cual llega” en una cadena de bloques no mejora la

confiabilidad: solo vuelve inmutable la inconsistencia. Por ello, antes del on-chain deben asegurarse estandarización semántica, validaciones automáticas, trazabilidad de fuentes y versionado de catálogos y reglas (Banco Interamericano de Desarrollo [BID], 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

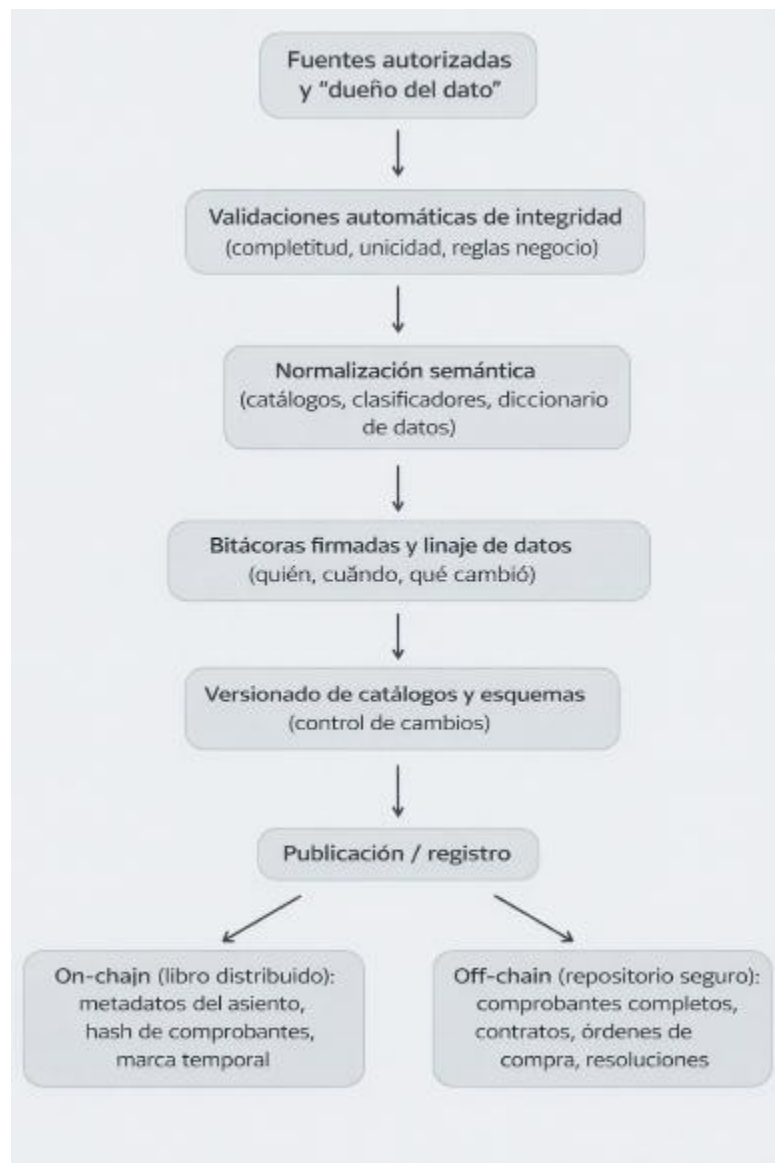
El BID enfatiza que el valor público no surge de la herramienta aislada, sino del diseño de gobernanza y del ciclo de datos. Es imprescindible definir quiénes generan, validan y consumen los datos, bajo qué reglas y con qué evidencia verificable, de modo que la publicación no exponga información sensible ni oculte lo indispensable para auditar (BID, 2020). A nivel nacional, los informes anuales de la Auditoría General de la Nación muestran que, aun con plataformas consolidadas como SIDIF, persisten inconsistencias, demoras de conciliación y faltantes de metadatos que dificultan el control oportuno, lo que obliga a fortalecer procedimientos de calidad e interoperabilidad antes de automatizar (Auditoría General de la Nación, 2022).

La Figura 28 esquematiza el pipeline de calidad e interoperabilidad previo al anclaje en blockchain, destacando fuentes autorizadas, validaciones y estandarización de datos.

Desde la perspectiva de control interno, el Marco COSO recuerda que la información debe ser pertinente, confiable, oportuna y accesible para apoyar los objetivos de control (COSO, 2013). Trasladado al diseño de un pipeline previo al anclaje en blockchain, ello implica: (a) fuentes autorizadas y con dueño de dato; (b) validaciones de integridad (completitud, unicidad, reglas de negocio, doble registro); (c) estándares de intercambio entre sistemas (por ejemplo, esquemas JSON/XML con catálogos cerrados de conceptos contables); (d) bitácoras firmadas digitalmente; y (e) metadatos que permitan reconstruir el linaje del asiento (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

INTOSAI señala que la obtención de evidencia suficiente y adecuada depende de la calidad de la información disponible y del acceso a los registros y sistemas pertinentes, lo que exige procedimientos adecuados de recolección y validación (INTOSAI, 2013). Si la organización no puede demostrar de dónde viene cada campo (origen) y quién lo transformó (linaje), la inmutabilidad de la cadena no sustituye la evidencia.

El control interno requiere que la información utilizada para apoyar su funcionamiento sea adecuada y de calidad, de manera que permita a la organización cumplir sus objetivos y responder a los riesgos que la afectan (COSO, 2013, p. 19).

Figura 28*Pipeline de calidad e interoperabilidad (antes del on-chain)*

Nota. Pipeline de calidad e interoperabilidad previo al on-chain. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); COSO (2013); INTOSAI (2013).

En la práctica, un pipeline de calidad previo al commit en la red debe incorporar controles ex ante (validaciones de negocio y conciliaciones locales) y controles ex post (reconciliaciones periódicas entre el libro distribuido y los ERP/fuentes origen). Además, conviene separar metadatos (on-chain) de documentos

completos (off-chain), referenciándolos con hashes y sellos de tiempo para asegurar verificabilidad sin exponer información sensible (BID, 2020). Esto alinea transparencia con confidencialidad y facilita auditorías selectivas: el auditor puede verificar el hash y solicitar el comprobante cuando corresponda, sin que el sistema publique en claro información protegida (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La Tabla 22 resume operativamente las etapas y controles del pipeline de calidad e interoperabilidad, indicando responsabilidades y puntos de verificación clave.

Un punto crítico de interoperabilidad es el significado contable. Sin un diccionario común (por ejemplo, catálogo de cuentas, clasificador del gasto, tipos de comprobante y estados de aprobación), cada sistema “habla” un idioma distinto. La solución típica es una capa de mapeos gobernada por una mesa interinstitucional (p. ej., OA–AGN–SIGEN–Hacienda) y esquemas de datos versionados: cuando cambia un catálogo, se emite una nueva versión y se mantiene el linaje. Este enfoque evita “romper” el libro cuando evoluciona la normativa o la estructura de cuentas.

Las reglas de negocio deben quedar documentadas y testeadas. Si luego se programan como contratos inteligentes, su lógica debe emanar de esos catálogos y reglas aprobadas (trazabilidad normativa → lógica de validación); de lo contrario, el riesgo es “codificar” un criterio no aprobado y, por tanto, no auditable, en tensión con los principios de INTOSAI sobre evidencia y documentación del trabajo (INTOSAI, 2013).

Como síntesis, un libro distribuido solo es tan bueno como su entrada de datos. Sin gobernanza de catálogos, validaciones sólidas y trazabilidad de transformaciones, la cadena consolida errores. Con calidad, normalización e interoperabilidad, en cambio, blockchain se vuelve un amplificador de confianza: el asiento no solo está íntegro y trazable, sino también explicable, reproducible y auditable (BID, 2020; COSO, 2013; INTOSAI, 2013; Auditoría General de la Nación, 2022).

Tabla 22
Pipeline de calidad e interoperabilidad (resumen operativo)

Etapa	Objetivo (resumen)	Responsable	Controles / Pruebas	Salida	Ubicación
Fuentes autorizadas	Cada campo desde sistema oficial con dueño del dato	Dueño del dato (Tesorería/Compras)	Listado de fuentes; actas; accesos controlados	Dataset por origen	Off
Validaciones automáticas	Detectar faltantes/duplicados y reglas de negocio	Equipo de datos + área funcional	Unit/ETL; reporte de errores; % calidad	Dataset validado	Off
Normalización semántica	Unificar catálogos y formatos	Mesa OA–AGN–SIGEN–Hacienda	Esquemas JSON/XML; diccionario versionado	Dataset normalizado	Off
Reglas pre-commit	Consistencia contable previa al registro	Contabilidad + Auditoría interna	Checks de saldos; conciliaciones firmadas	Asientos prevalidos	Off
Bitácoras y linaje	Trazar quién/qué/cuándo en el pipeline	TI + Seguridad	Logs firmados; hash; trazabilidad	Bitácoras con hash	Off
Versionado	Mantener compatibilidad y trazas de cambio	Gobernanza de datos	Historial de versiones; diffs aprobados	Catálogos/esquemas vN	Off
Publicación on-chain	Huella de asientos y comprobantes	Nodos del consorcio	Tx con metadatos + hash; timestamp	Asiento anclado (txid)	On
Repositorio off-chain	Conservar comprobantes íntegros y controlados	Archivo/Legales + TI	Accesos; auditoría de descargas; retención	Docs vinculados por hash	Off

Nota. Valores cualitativos orientativos; la implementación concreta depende de los catálogos y procesos de cada organismo. Adaptado de Banco Interamericano de Desarrollo (2020), COSO (2013) e INTOSAI (2013).

3.5.3 Gobernanza, responsabilidades y control interno

En redes donde participan varios organismos —por ejemplo, OA, AGN, SIGEN y Hacienda— resulta imprescindible definir con precisión la gobernanza del consorcio: quién opera y mantiene nodos, cómo se incorporan o expulsan validadores, qué mayorías se exigen para modificar parámetros de la red o actualizar contratos inteligentes y de qué modo se auditan las claves criptográficas y los registros de cambio. La orientación internacional converge en priorizar acuerdos explícitos de membresía, reglas de decisión documentadas y segregación de funciones para asegurar trazabilidad y rendición de cuentas (Banco

Interamericano de Desarrollo [BID], 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La Figura 29 muestra el flujo de gobernanza del consorcio, incluyendo decisiones sobre membresía, operación de nodos y gestión de cambios en la red.

Desde la perspectiva de control interno, el Marco COSO subraya que el diseño de actividades de control debe incluir autorizaciones, verificaciones independientes y segregación de funciones a fin de mitigar riesgos de error o fraude.

La segregación de funciones constituye un principio clave para reducir las oportunidades de actos indebidos al distribuir las responsabilidades entre distintos individuos y áreas (COSO, 2013, secc. Actividades de control).

Figura 29

Diagrama de flujo de gobernanza del consorcio



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

En el mismo sentido, INTOSAI recalca que la auditoría del sector público requiere “evidencia suficiente y adecuada para sustentar conclusiones”, lo que demanda registros completos, accesibles y

protegidos frente a alteraciones (INTOSAI, 2013, secc. Evidencia). La Tabla 23 detalla la matriz RACI de gobernanza, asignando responsables, aprobadores, consultados e informados para cada actividad crítica de la red.

Tabla 23

RACI de gobernanza (roles por actividad)

Actividad de gobernanza	OA	AGN	SIGEN	Hacienda	TI del Consorcio	Auditoría interna	Auditoría externa
Admisión/suspensión/retiro de miembros	A	C	C	R	R	C	I
Operación de nodos validadores	A	C	C	R	R	C	I
Gestión de claves (HSM, multifirma, rotación)	A	C	C	R	R	C	I
Despliegue/actualización de contratos inteligentes	A	C	C	R	R	C	I
Gestión de cambios de parámetros de red	A	C	C	R	R	C	I
Monitoreo y observabilidad (métricas/alertas)	A	C	C	R	R	C	I
Auditoría periódica de nodos y contratos	A	C	C	R	R	C	I
Respuesta a incidentes y contingencias	A	C	C	R	R	C	I

Nota. Responsable (R), Aprobador (A), Consultado (C) e Informado (I) por actividad clave. Valores orientativos; la RACI final debe formalizarse por estatuto y políticas del consorcio. Elaboración propia a partir de Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Más allá de los enunciados, la gobernanza eficaz se concreta en mecanismos operativos. Primero, la gestión del ciclo de vida de la membresía: admisión, suspensión y retiro de entidades; requisitos de identidad y cumplimiento; publicación de un registro auditable de decisiones. Segundo, políticas de

custodia de claves y operaciones críticas: uso de HSM, controles de múltiples firmas para acciones sensibles (por ejemplo, desplegar contratos o modificar parámetros), recuperación y rotación con evidencias verificables. Tercero, procedimientos de cambio (change management) con propuesta, revisión, votación y ejecución on-chain/off-chain, incluyendo ventanas de mantenimiento, reversión segura ante fallas y actas firmadas digitalmente. Cuarto, observabilidad y trazabilidad: bitácoras inmutables de operación, métricas de salud de la red, alertas y auditorías periódicas, con responsables nominados y planes de respuesta a incidentes (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La literatura aplicada a contratación pública con blockchain enfatiza que el valor no proviene del registro por sí solo, sino de reglas claras y exigibles.

El consorcio debe acordar y publicar reglas de membresía, responsabilidades y procedimientos de toma de decisión; la tecnología es condición necesaria, pero el valor público proviene de la gobernanza —quién decide, cómo y con qué controles— y de su cumplimiento verificable (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, secc. Recomendaciones).

Para alinear blockchain con control interno, conviene mapear los cinco componentes de COSO a controles específicos:

Ambiente de control: estatuto del consorcio, código de ética, atribución formal de roles (dueños de proceso, administradores de nodo, custodios de claves).

Evaluación de riesgos: matriz de riesgos técnicos y administrativos (p. ej., colusión de validadores, fuga de claves, cambios no autorizados) con respuestas y responsables.

Actividades de control: políticas de despliegue de contratos con revisión independiente, multifirma para cambios críticos, segregación entre quienes desarrollan, aprueban y operan.

Información y comunicación: tableros de monitoreo, actas y reportes periódicos a órganos de control, repositorios de configuración y versiones.

Monitoreo: auditorías internas/externas, pruebas de efectividad de controles, remediación de hallazgos (COSO, 2013; INTOSAI, 2013).

Además, cuando varias entidades validan bloques, la “inmutabilidad” debe ser también institucional: no basta con que el protocolo dificulte reescrituras; es necesario que nadie pueda imponer cambios sin cumplir el procedimiento acordado. Por ello se recomiendan umbrales de votación (p. ej., 2/3 BFT) para operaciones sensibles, junto con registros firmados de cada decisión y mecanismos de no repudio sobre acciones administrativas (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; BID, 2020).

Una red de consorcio orientada a contabilidad pública solo crea confianza si la gobernanza es clara, documentada y auditable: reglas de membresía, segregación de funciones, controles de claves, gestión de cambios, monitoreo continuo y un canal institucional para la auditoría. COSO aporta el marco para

estructurar los controles, INTOSAI fija el estándar de evidencia y Foro Económico Mundial & Banco Interamericano de Desarrollo brindan guías de implementación sectorial. La Tabla 24 ejemplifica umbrales de votación para acciones sensibles en la red.

Tabla 24

Umbrales de votación para acciones sensibles

Acción sensible	Umbral sugerido (BFT)	Evidencia requerida
Admisión/suspensión de miembro	$\geq 2/3$ de validadores	Acta firmada digitalmente; registro on-chain de la votación
Cambio de parámetros críticos de consenso	$\geq 2/3$ de validadores	Registro on-chain; prueba de tests; ventana de mantenimiento
Despliegue de contrato que impacta ejecución del gasto	$\geq 2/3$ de validadores y revisión independiente	Bitácora de revisión; hash del artefacto; resultado de votación
Rotación/recuperación de claves maestras	$\geq 3/4$ de validadores y doble control (multifirma)	Bitácora HSM; registro de custodios; evidencia de recuperación
Parada/arranque de la red o de un canal	$\geq 3/4$ de validadores, con acta y plan de contingencia	Acta y notificación; métricas de impacto; aprobación de contingencia

Nota. Elaboración propia basada en Banco Interamericano de Desarrollo (2020); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); COSO (2013); INTOSAI (2013).

3.5.4 Privacidad, confidencialidad y acceso a la información

Publicar asientos verificables sin exponer datos sensibles exige separar con criterio qué se registra en la cadena (metadatos, hashes, estados) y qué permanece fuera (documentos completos, datos personales o comerciales). El Banco Interamericano de Desarrollo advierte que los proyectos de blockchain en el sector público deben diseñar “reglas claras de manejo de datos, minimización de exposición y segmentación por sensibilidad” (BID, 2020, secc. Gobernanza de datos). El qué y el cómo de la publicación no son un asunto meramente técnico: definen el riesgo regulatorio y reputacional de la institución.

El marco normativo argentino obliga a equilibrar transparencia y protección de datos. La Ley 27.275 reconoce el acceso a la información pública como regla, pero habilita excepciones cuando su divulgación afectaría derechos protegidos o secretos legalmente establecidos (Ley 27.275, 2016). A la vez,

la Ley 25.326 exige principios de licitud, finalidad, calidad y seguridad para el tratamiento de datos personales, lo que implica limitar su circulación y adoptar medidas de resguardo (Ley 25.326, 2000). En términos prácticos, esto se traduce en clasificar datos por sensibilidad, publicar comprobantes criptográficos (hashes y sellos de tiempo) y ofrecer vistas agregadas que no permitan reidentificación por correlación.

La Figura 30 representa el flujo de publicación con privacidad, desde la clasificación de datos hasta la decisión sobre qué se mantiene off-chain y qué se ancla on-chain.

De acuerdo con lineamientos internacionales, conviene aplicar estrategias complementarias: pseudonimización de identificadores, canales privados o particiones de datos en redes permissionadas, cifrado a nivel de campo y, cuando corresponda, pruebas de conocimiento cero para demostrar cumplimiento de reglas sin revelar los valores subyacentes (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). El BID sintetiza el enfoque con una recomendación operativa clara: “no toda la información debe incorporarse en la cadena; es preferible almacenar referencias verificables y preservar el contenido detallado en repositorios gestionados con control de acceso” (BID, 2020, secc. Diseño de datos).

La adopción responsable de blockchain en el sector público requiere políticas explícitas de clasificación y minimización de datos, mecanismos de control de acceso y trazabilidad de responsabilidades sobre quién ve qué y cuándo. El objetivo es maximizar la verificabilidad pública sin comprometer derechos individuales ni secretos protegidos; para ello, las soluciones híbridas (registro on-chain de evidencias y resguardo off-chain de contenidos sensibles) resultan especialmente adecuadas (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, secc. Recomendaciones). La Tabla 25 organiza, en forma de matriz, qué elementos conviene registrar on-chain y cuáles deben resguardarse off-chain, junto con su fundamento jurídico.

Figura 30*Flujo de publicación con privacidad*

Nota. El diagrama representa el recorrido “ingesta → calidad/normalización → clasificación sensible/no sensible → publicación on-chain/off-chain”, con anclaje público de hashes y registro de auditoría de accesos y cambios. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Tabla 25*Matriz on-chain/off-chain y base legal*

Dato	Sens.	Base legal (AR)	Almacenamiento	Acceso	Retención
ID de asiento (UUID)	Baja	Ley 27.275 (publicidad)	OC en claro	Público	Permanente
Fecha y tipo de operación	Baja	Ley 27.275 (publicidad)	OC en claro	Público	Permanente
Monto y moneda	Media	Ley 27.275 (difusión agregada)	OC agregado; detalle OF + hash	Público agregado / interinst.	Según normas contables
CUIT / ID proveedor	Alta	Ley 25.326 (dato personal)	OF con control + hash OC	Interinst./Restringido	Según régimen de datos personales
Documento respaldatorio (PDF)	Alta	Ley 25.326; exc. Ley 27.275	OF seguro + hash/timestamp OC	Interinst./Restringido	Según archivo/contrataciones
Estado de aprobación (workflow)	Baja–Media	Ley 27.275 (transparencia)	OC en claro	Público	Histórico
CBU / cuenta bancaria	Alta	Ley 25.326 (sensibles)	OF cifrado + hash OC	Restringido	Según tesorería
Detalle de bienes/servicios	Media	Ley 27.275 (posible publicidad)	OC resumen; detalle OF + hash	Público (agregado) / interinst.	Según contratación
Observaciones internas	Alta	Ley 27.275 (secreto adm.)	OF con control + hash OC	Restringido	Según norma interna
Contrato / pliego	Variable	Ley 27.275 (pub./exc.)	OF completo + hash OC	Público / interinst.	Según contratación
ID de expediente	Media	Ley 27.275 (publicidad)	OC en claro	Público	Histórico
Usuario responsable (rol)	Media	Ley 25.326	OC por rol/pseud.; identidad OF	Interinst./Restringido	Según RR.HH. y auditoría

Nota. La asignación de elementos a on-chain (metadatos, estados, hashes y sellos de tiempo) u off-chain (documentos completos, datos personales y comerciales) se fundamenta en los principios de acceso a la información pública (Ley 27.275, 2016) y de protección de datos personales (Ley 25.326, 2000), complementados por guías técnicas sobre segmentación y minimización de datos en soluciones blockchain para el sector público (Banco Interamericano de Desarrollo, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

El control interno también debe alinearse con estos principios. COSO (2013) enfatiza que el ambiente de control incluye políticas y procedimientos para salvaguardar información; en un libro

distribuido, esto implica gobernar llaves criptográficas, definir perfiles y auditorías de acceso y documentar las reglas de publicación de datos (COSO, 2013). Asimismo, INTOSAI recuerda que la evidencia debe ser “suficiente y apropiada” (ISSAI 100) y su obtención no puede vulnerar restricciones legales de confidencialidad (INTOSAI, 2013). La trazabilidad criptográfica, por tanto, no reemplaza a la gobernanza documental: la complementa.

La Tabla 26 compara distintas técnicas de privacidad aplicables a entornos blockchain gubernamentales, considerando su alcance, desempeño y riesgos de reidentificación.

Desde una perspectiva operativa, resulta recomendable adoptar un esquema de minimización (publicar solo lo necesario para verificar integridad y estados), desagregación temporal (por ejemplo, publicación diferida de ciertos metadatos para evitar riesgos de mercado o seguridad) y capas de acceso (vistas públicas, interinstitucionales y restringidas) con registros de auditoría sobre cada consulta. El resultado buscado es una transparencia verificable que permita a terceros comprobar integridad y consistencia sin acceder a datos sensibles ni reidentificables.

La Figura 31 presenta un modelo de capas de acceso, diferenciando vistas públicas, interinstitucionales y restringidas sobre los mismos registros contables.

En suma, la privacidad en contabilidad pública basada en blockchain se protege combinando diseño de datos (on-chain/off-chain), controles criptográficos (hashes, firmas, pruebas de conocimiento cero), gobernanza de acceso y cumplimiento normativo. El objetivo es doble: maximizar la auditoría social e interinstitucional y, al mismo tiempo, cumplir con la Ley 27.275 y la Ley 25.326, asegurando que la integridad verificable no se logre a costa de la confidencialidad.

Tabla 26
Comparativa de técnicas de privacidad aplicables

Técnica	Propósito	Ventajas	Limitaciones	Costo/Complejidad	Adecuación sector público
Pseudonimización	Evitar identificación directa	Simple y reversible bajo control	No protege ante correlación	Media	Alta (con gobernanza de llaves)
Cifrado por campo	Ocultar valores sensibles	Granular y compatible con repositorios	Gestión de llaves crítica	Media	Alta
Canales privados/particiones	Segregar datos por sensibilidad	Control fino de acceso	Complejidad operativa en consorcios	Media-Alta	Alta
Hash + timestamp	Probar integridad sin revelar contenido	Sencillo y auditable	No oculta metadatos	Baja	Alta
Pruebas de conocimiento cero (ZK)	Verificar reglas sin exponer datos	Privacidad fuerte	Desarrollo y verificación costosos	Alta	Media (casos críticos)
Publicación diferida	Mitigar riesgos temporales	Reduce exposición inmediata	Demora transparencia en tiempo real	Baja	Media-Alta (según proceso)
Control de acceso por roles/atributos (RBAC/ABAC)	Restringir vistas según necesidad	Compatible con auditoría	Requiere gobierno de identidades	Baja-Media	Alta
Registros de acceso firmados	No repudio y trazabilidad	Facilita auditoría	Almacenamiento y revisiones periódicas	Baja	Alta

Nota. La tabla resume alcances y limitaciones de pseudonimización, cifrado a nivel de campo, canales privados/particiones, hash + timestamp y pruebas de conocimiento cero en contextos gubernamentales, considerando desempeño, verificabilidad y riesgo de reidentificación. Adaptado de Foro Económico Mundial & Banco Interamericano de Desarrollo (2020) y Banco Interamericano de Desarrollo (2020), con aportes sobre implicancias contables de contratos inteligentes en Santos (2022).

Figura 31*Modelo de capas de acceso*

Nota. El modelo separa vistas públicas (metadatos y estados agregados), vistas interinstitucionales (detalles operativos sujetos a convenio) y vistas restringidas (datos sensibles), indicando artefactos on-chain (hashes, estados, marcas de tiempo, eventos) y off-chain (documentos íntegros en repositorios con control de acceso). Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020), Foro Económico Mundial & Banco Interamericano de Desarrollo (2020) y en los principios de información y comunicación del marco COSO (2013).

3.5.5 Finalidad, rendimiento y continuidad operativa

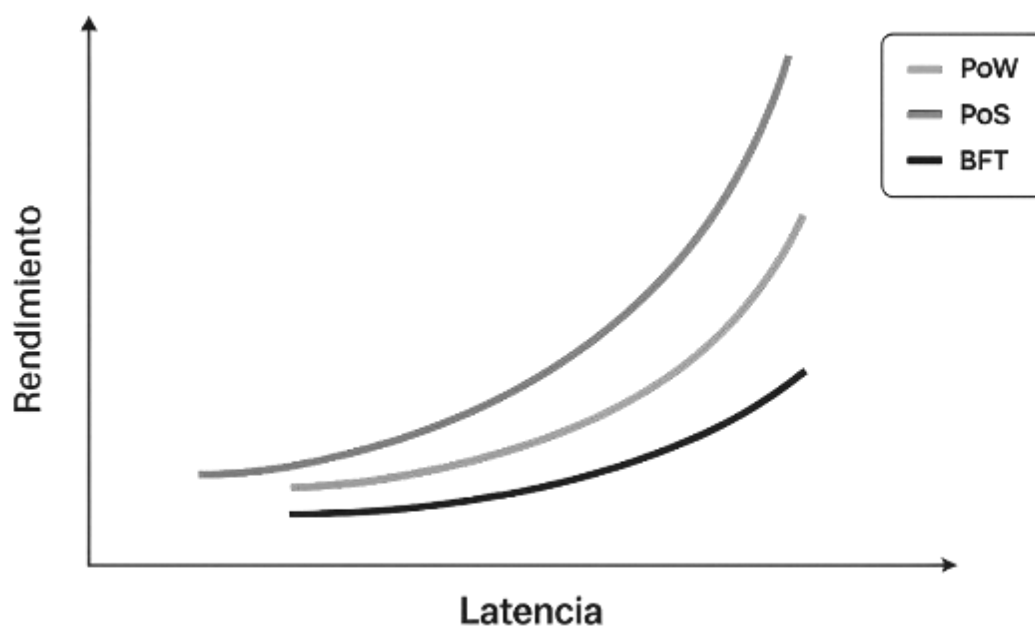
La contabilidad gubernamental exige cierres, cortes y conciliaciones con finalidad clara: certeza práctica de que un asiento no se revertirá. En redes abiertas basadas en prueba de trabajo, la finalidad es probabilística y crece con la profundidad de confirmaciones. Como señaló Nakamoto, “We propose a solution to the double-spending problem using a peer-to-peer network” (2008, secc. 1), lo que supone que la irreversibilidad aumenta a medida que la cadena honesta avanza y hace económicamente inviable la reescritura del historial por parte de un atacante. En proyectos públicos, esa incertidumbre residual obliga a definir políticas de cierre (por ejemplo, número mínimo de confirmaciones por tipo de asiento) y ventanas temporales de consolidación contable (BID, 2020).

Los entornos permissionados que emplean consensos tolerantes a fallos bizantinos (p. ej., PBFT/IBFT) proveen finalidad práctica en segundos: cuando el bloque es aceptado por el quórum de validadores, se considera final, lo que se ajusta mejor a los hitos operativos de tesorería, compras y cierre

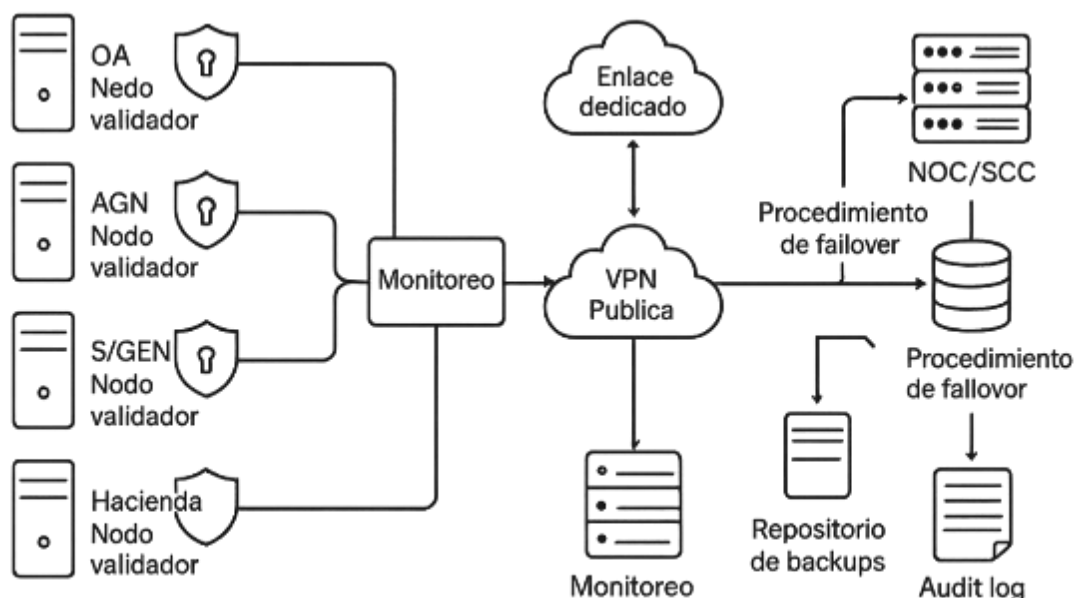
mensual (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Esta ventaja tiene condiciones: identidades fuertes, operación coordinada de nodos y procedimientos de alta disponibilidad. La guía del BID y del Foro Económico Mundial sugiere que la selección del consenso debe responder a objetivos de servicio (SLA), perfiles de carga y requisitos de auditoría, evitando adoptar modelos abiertos solo por “prestigio tecnológico” si la finalidad rápida y determinista es un requisito funcional (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La capacidad de procesamiento (throughput) y la latencia dependen tanto del consenso como del diseño de contratos inteligentes. En palabras de Wood, “Ethereum is a transaction-based state machine” (2014, secc. 1), de modo que cada validación contable consume recursos en la máquina de estados, y un exceso de lógica on-chain puede introducir cuellos de botella. La documentación del BID advierte que el desempeño debe modelarse antes de producción, con pruebas de carga y límites de gas/cuotas adecuados (BID, 2020). En términos prácticos, conviene mantener en cadena los metadatos (hashes, estados, firmas, marcas de tiempo) y relegar a repositorios externos los documentos completos, combinando referencias verificables con pipelines de calidad y cacheo de lecturas para reportes. La Figura 32 ilustra, de forma conceptual, la relación entre rendimiento y latencia para distintos tipos de consenso utilizados en redes blockchain.

Respecto de la continuidad operativa, los lineamientos internacionales indican que las redes públicas confían la disponibilidad a la resiliencia masiva de nodos globales, mientras que las permissionadas requieren una ingeniería explícita: múltiples validadores en distintos dominios organizacionales, balanceo, monitoreo, restauración ante desastres y rotación segura de claves (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La evidencia de INTOSAI sugiere además que la oportunidad y la confiabilidad de la información son atributos esenciales de la evidencia de auditoría; por tanto, la infraestructura debe sostener niveles de servicio compatibles con calendarios presupuestarios y cierres (INTOSAI, 2013). La Figura 33 esquematiza una arquitectura de continuidad operativa para una red permissionada orientada a contabilidad pública, con validadores distribuidos y mecanismos de respaldo.

Figura 32*Curvas conceptuales rendimiento-latencia*

Nota. Curvas conceptuales rendimiento-latencia: tres curvas lisas etiquetadas “PoW”, “PoS” y “BFT” muestran tendencias relativas (PoW: menor rendimiento y mayor latencia; BFT: mayor rendimiento y menor latencia; PoS: comportamiento intermedio Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Wood (2014).

Figura 33*Arquitectura de continuidad operativa en red permissionada*

Nota. Validadores distribuidos entre OA, AGN, SIGEN y Hacienda; HSM por nodo; monitoreo central; canal de contingencia y procedimiento de failover. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) e INTOSAI (2013).

A efectos de orientar decisiones, resulta útil fijar umbral de finalidad por tipo de operación (p. ej., órdenes de pago vs. ajustes contables), modelar escenarios de falla (pérdida de un validador, partición de red, rotura de HSM), y ensayar procedimientos de recuperación documentados. La experiencia recogida en el sector público latinoamericano recomienda también separar redes de pre-producción para pruebas funcionales y de seguridad, con datos sintéticos y scripts de verificación automática (BID, 2020).

Para contextos de gestión pública, la finalidad operativa debe entenderse como un contrato de servicio entre áreas usuarias y la red: reglas claras sobre cuándo un asiento puede considerarse definitivo, qué condiciones de quórum y consenso lo habilitan, y cómo se procede ante fallas, particiones o eventos de seguridad. Diseñar estos parámetros por adelantado reduce la discrecionalidad y favorece auditorías oportunas (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, secc. Recomendaciones).

Resumiendo, la finalidad en blockchain no es un atributo único: varía por consenso y por configuración; el rendimiento depende del equilibrio entre lógica on-chain y off-chain; y la continuidad exige ingeniería y gobernanza específicas. Las redes permissionadas con BFT suelen alinearse mejor con

los ritmos de la contabilidad pública, siempre que se acompañen de identidades robustas, alta disponibilidad y políticas de cierre bien definidas (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Nakamoto, 2008; Wood, 2014; INTOSAI, 2013).

3.5.6 Evidencia, auditoría y nuevos procedimientos

La auditoría en entornos con blockchain exige traducir principios clásicos —suficiencia, idoneidad y oportunidad de la evidencia— a un soporte criptográfico compuesto por hashes, firmas digitales, pruebas de inclusión (Merkle proofs) y registros de eventos de contratos inteligentes. En términos prácticos, las pruebas sustantivas y de cumplimiento deben rediseñarse para validar, por un lado, la integridad del rastro (encadenamiento y huellas criptográficas) y, por otro, la eficacia de los controles programados (reglas on-chain que ejecutan aprobaciones, límites, segregación de funciones y anulación justificada) (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Como sintetiza INTOSAI, “la evidencia de auditoría” ha de ser “suficiente y apropiada” para sustentar conclusiones (INTOSAI, 2013, ISSAI 100).

En el plano operativo, el rastro on-chain solo resulta auditable si el puente con los sistemas fuente (compras, tesorería, patrimonio) garantiza exactitud y completitud. Los lineamientos del BID y del Foro Económico Mundial sugieren implementar tuberías de datos firmadas, validaciones de negocio antes del alta en cadena, y catálogos consistentes que permitan conciliar automáticamente asientos, comprobantes y estados de contrato; sin esa capa, la inmutabilidad de la cadena preserva errores en lugar de corregirlos (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). En paralelo, la literatura contable observa que el uso de libros distribuidos reduce tiempos y costos de auditoría cuando la trazabilidad es completa y estandarizada, a la vez que reconfigura la evaluación de riesgos hacia la fiabilidad del diseño y la operación de controles automatizados (Morales, 2021; Santos, 2022).

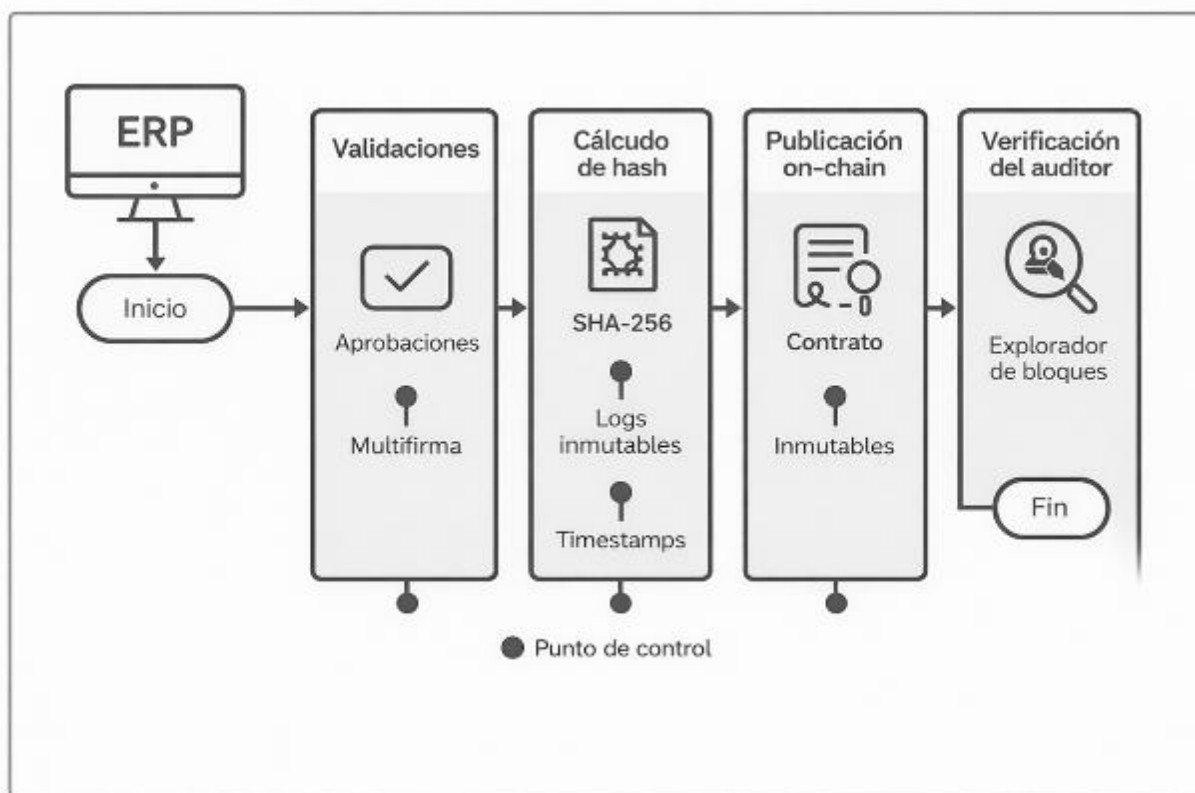
Un enfoque de auditoría para cadenas de bloques en el sector público debe especificar los objetos de evidencia (transacciones, eventos, estados), los criterios de verificación (integridad, existencia, autorización), los procedimientos para reproducir pruebas criptográficas y los mecanismos de muestreo y reconciliación con sistemas externos. La ganancia de eficiencia dependerá de la calidad del diseño y de la disciplina operativa de los participantes del consorcio (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, Recomendaciones).

Bajo este marco, la evidencia criptográfica opera como equivalente funcional de sellos y firmas manuales, con ventajas de verificabilidad independiente: un auditor puede recalcular el hash de un comprobante y cotejarlo con el publicado en bloque; puede probar inclusión de una transacción por su ruta Merkle; y puede reconstruir la secuencia de aprobaciones leyendo los event logs de contratos. COSO enfatiza la relevancia de “segregación de funciones, autorización, registros y supervisión” como pilares de

control (COSO, 2013), lo que en blockchain se traduce en roles y permisos on-chain, políticas de firma (p. ej., multifirma) y controles ex ante programables. La Figura 34 describe la cadena de custodia digital de los comprobantes, desde su generación hasta la verificación de integridad mediante artefactos criptográficos.

Figura 34

Cadena de custodia digital



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

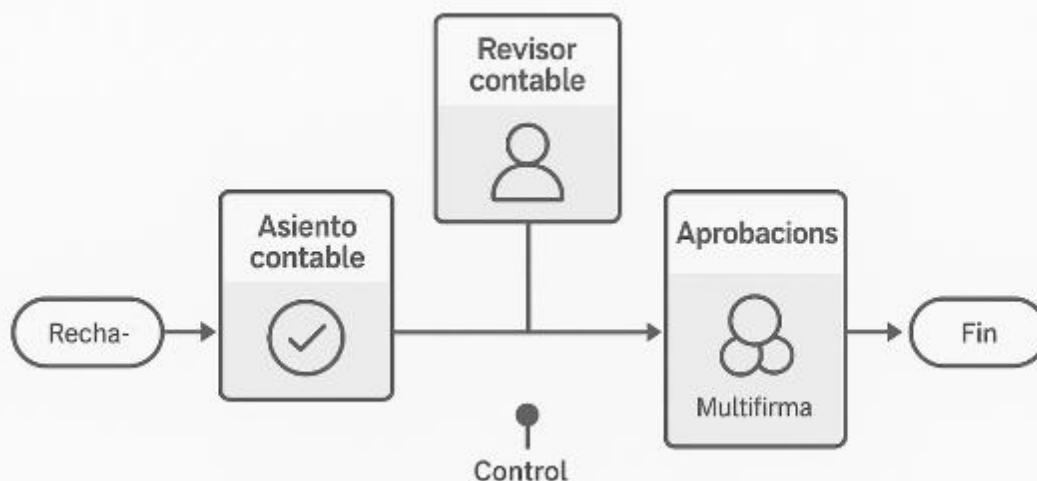
La adopción trae consigo nuevos procedimientos: (a) pruebas de calidad de datos del pipeline (completitud, unicidad, coherencia entre ERP y cadena); (b) re-ejecución determinista de funciones críticas de contratos para verificar resultados esperados; (c) verificación de parametría (umbrales, listas de autorizantes, calendarios de cierre); (d) revisión de gestión de claves (custodia HSM, rotación, revocación, recuperación); y (e) análisis de configuraciones de consenso (quórum, tolerancia a fallos) y su impacto en finalidad y oportunidad de evidencia (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). INTOSAI recuerda que la evidencia debe ser “oportuna y pertinente” para apoyar las

conclusiones del auditor (2013, ISSAI 100), de modo que los SLA de la red y de los conectores con sistemas legados son, en sí mismos, materia de auditoría.

También cambia el enfoque de muestreo. En registros tradicionales, el auditor compensa la opacidad con técnicas de muestreo representativo; en registros distribuidos, la consulta total (audit analytics) resulta factible para muchos procedimientos, pero requiere herramientas que preserven el valor probatorio del rastro (cadenas de custodia, consultas reproducibles, registros de auditor). La literatura sugiere que el énfasis se desplaza desde “ver unos pocos asientos” hacia verificar la corrección sistemática de reglas y flujos, respaldado por pruebas criptográficas que acreditan que ningún participante alteró el historial sin dejar evidencia (Morales, 2021; Santos, 2022).

En términos de capacidades, se vuelve indispensable capacitar equipos públicos y auditores externos en lectura e interpretación de trazas on-chain, reproducción de pruebas criptográficas, y forense de contratos (decodificación de eventos, análisis de estados, detección de reentradas o desbordes). El BID recomienda alinear los proyectos con “objetivos públicos verificables y medibles” (BID, 2020, Criterios de selección), lo que en auditoría se traduce en indicadores de calidad de evidencia (porcentaje de asientos con hash verificable, latencia promedio de publicación, tasa de conciliaciones automáticas, cobertura de controles ex ante).

Por último, integrar control interno y auditoría externa sobre un mismo libro distribuido redundante en un circuito virtuoso: controles programados que previenen, bitácoras inmutables que disuaden, y evidencia autosuficiente que acelera la verificación. Los beneficios potenciales —integridad verificable, reducción de tiempos y trazabilidad exhaustiva— dependen de gobernanzas claras, datos estandarizados y competencias específicas en criptografía aplicada y análisis de cadenas (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; COSO, 2013; INTOSAI, 2013; Morales, 2021; Santos, 2022). La Figura 35 muestra un mapa de competencias necesarias para auditar entornos blockchain, articulando conocimientos contables, normativos y técnicos.

Figura 35*Mapa de competencias para auditoría blockchain*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en INTOSAI (2013), COSO (2013) y Morales (2021).

3.5.7 Integración con sistemas legados y continuidad documental

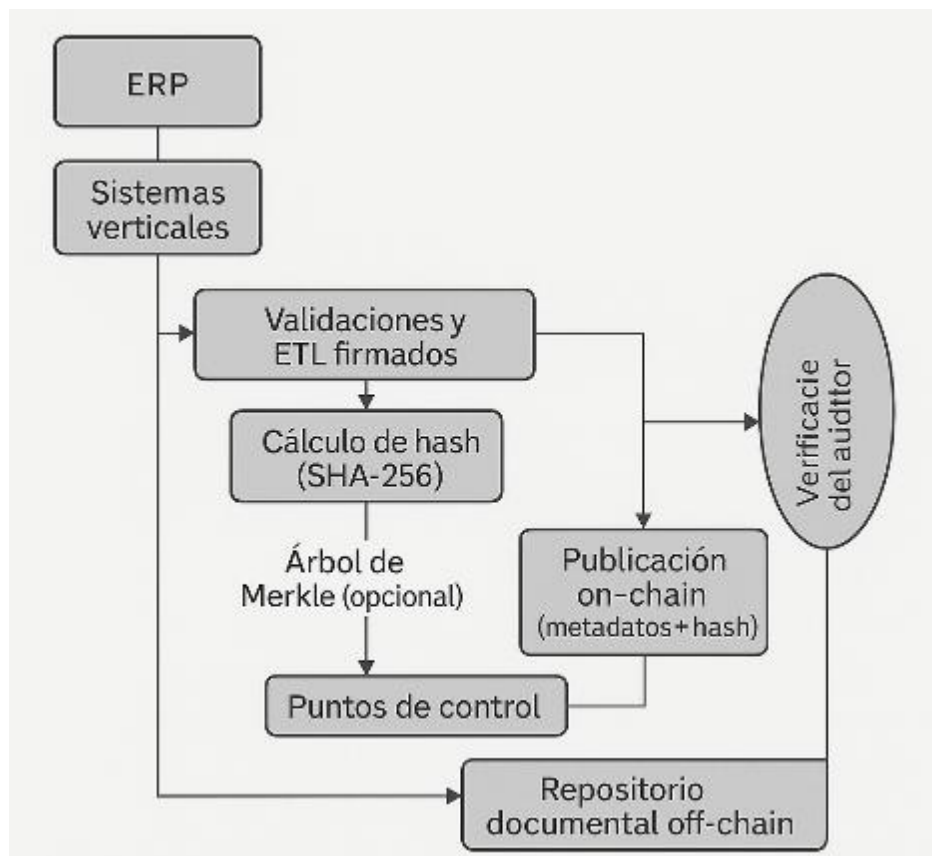
En la práctica, los asientos contables del Estado se originan en sistemas fuente —ERP financieros y verticales de compras, tesorería, patrimonio e inventarios— que seguirán operando y que, por lo tanto, deben integrarse con la red blockchain sin duplicaciones, sin rupturas de trazabilidad y sin pérdida de valor probatorio. El Banco Interamericano de Desarrollo lo sintetiza al indicar que el valor público depende de “reglas de intercambio y auditoría claramente definidas” (Banco Interamericano de Desarrollo [BID], 2020, secc. Gobernanza de datos). De allí que la arquitectura de integración requiera APIs autenticadas y firmadas, procesos ETL/ELT con controles de calidad y un modelo canónico de datos que permita mapear, de forma determinista, cada asiento y su comprobante hacia estructuras on-chain y referencias off-chain (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

En un esquema viable para la administración pública, los documentos completos (órdenes de compra, facturas, contratos, expedientes) permanecen en repositorios seguros fuera de la cadena (off-chain), mientras que metadatos críticos —fecha, importe, clasificadores presupuestarios, referencias de expediente, identidad de autorizantes— y los hashes de cada comprobante se publican en la cadena (on-chain). Con este patrón, cualquier auditor puede recalcular el hash del documento original y cotejarlo con el anclado en blockchain, cerrando así el circuito de cadena de custodia (BID, 2020). Además, la firma digital de los mensajes de integración evita manipulaciones en tránsito y contribuye a la autenticidad y no repudio de los asientos; INTOSAI recuerda que la evidencia debe ser “suficiente y apropiada” para sustentar conclusiones

(INTOSAI, 2013, ISSAI 100), y esos atributos incluyen la confiabilidad del canal que transporta los datos. La Figura 36 muestra la arquitectura propuesta de integración y cadena de custodia, articulando sistemas fuente, repositorios off-chain y anclaje on-chain de evidencias.

Figura 36

Arquitectura de integración y cadena de custodia



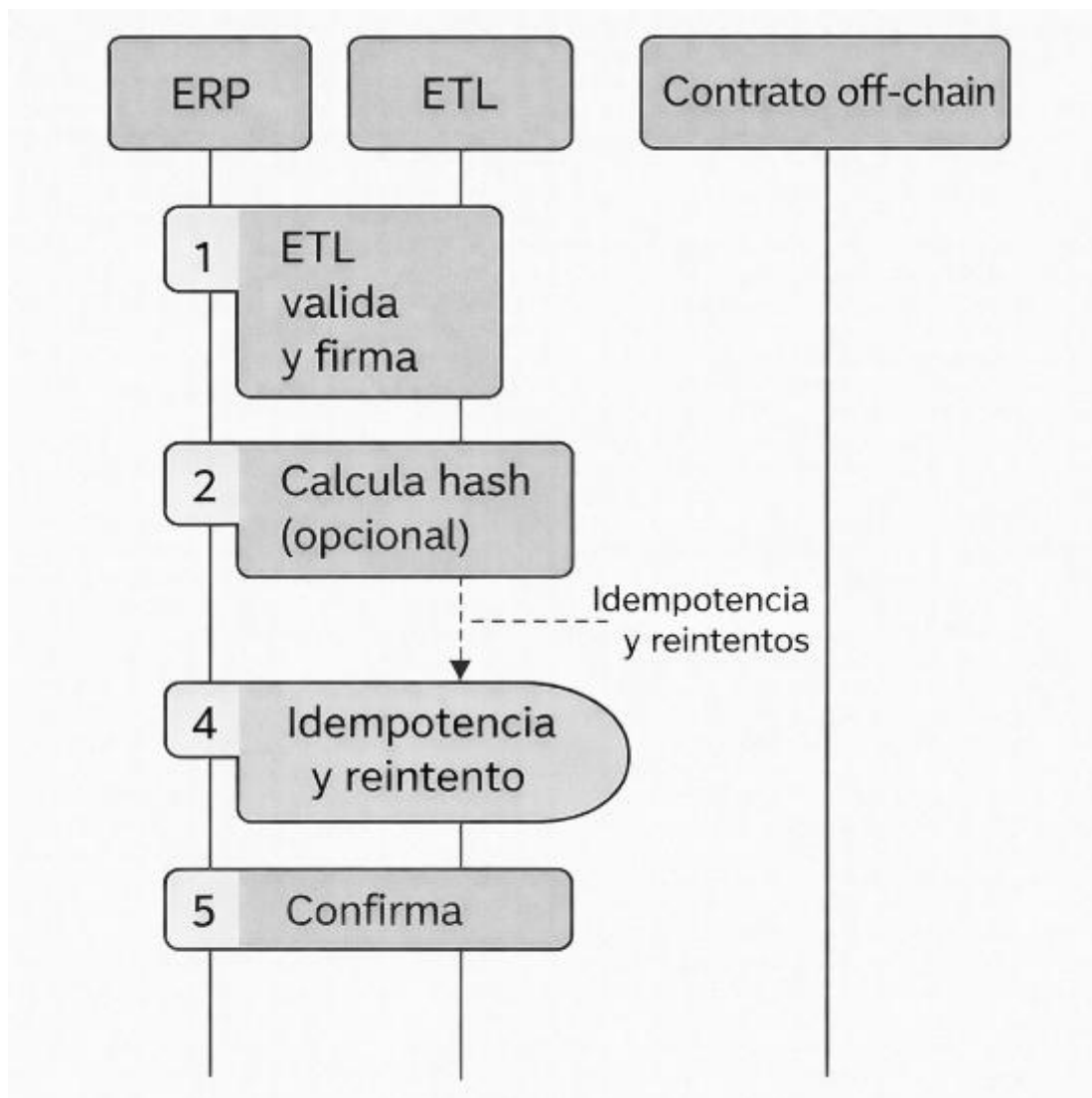
Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

La integración debe contemplar validaciones ex ante (reglas de negocio y de integridad referencial antes del alta en cadena), versionado de esquemas y transformaciones, y registros de auditoría que documenten quién, cuándo y bajo qué parámetros ejecutó cada carga. A nivel operativo, conviene emplear identificadores canónicos (por ejemplo, UUIDs) y catálogos controlados (clasificadores presupuestarios, unidades ejecutoras, proveedores) para evitar divergencias semánticas entre sistemas; sin esa disciplina, la inmutabilidad de la cadena preservará errores en lugar de corregirlos (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La interoperabilidad efectiva en el sector público exige estandarizar catálogos y metadatos, garantizar que las transformaciones sean reproducibles, firmar digitalmente los mensajes de sistema a sistema y publicar en la cadena únicamente la evidencia necesaria (hashes, marcas de tiempo, referencias) para preservar confidencialidad. La continuidad documental se logra alineando políticas de retención y acceso con la infraestructura técnica (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, Recomendaciones).

En paralelo, la continuidad documental obliga a definir políticas de retención y preservación que abarquen tanto el repositorio off-chain (documentos completos) como la evidencia on-chain (hashes, marcas de tiempo y eventos de contratos). COSO subraya, en clave de control interno, la importancia de la segregación de funciones, la autorización y la documentación como pilares del registro fiable (COSO, 2013), lo que en este contexto se traduce en flujos de aprobación programables (smart contracts) y en roles con permisos mínimos necesarios (principio de least privilege). A nivel normativo, la validez jurídica de la evidencia digital se refuerza con la utilización de firmas digitales conforme a la Ley 25.506, que en Argentina reconoce su equivalencia funcional con la firma ológrafa para conferir autoría e integridad a los documentos electrónicos (Ley 25.506, 2001). La Figura 37 describe una secuencia de integración idempotente, en la que cada intento de registro produce el mismo resultado contable y de evidencia, evitando duplicidades y errores.

Figura 37
Secuencia de integración idempotente



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020).

La Auditoría General de la Nación observa que, aun con plataformas como SIDIF, persisten “inconsistencias y dificultades de conciliación” que demandan fortalecer normalización e interoperabilidad antes de automatizar (Auditoría General de la Nación, 2022). Esto justifica que el pipeline de integración incluya controles de calidad de datos (completitud, unicidad, coherencia temporal), conciliaciones

automáticas entre ERP y cadena, y alarmas cuando un asiento carezca del hash o cuando el hash no verifique contra el documento almacenado.

Desde el punto de vista de continuidad operativa, la integración ha de ser resiliente: colas de mensajería con reintentos idempotentes, partición de cargas por dominios (compras, pagos, contrataciones) y monitoreo de latencia entre evento en el ERP y anclaje on-chain. Además, los contratos inteligentes deberían rechazar transacciones cuando el estado del catálogo (p. ej., proveedor inhabilitado, partida presupuestaria agotada) no sea el esperado, registrando eventos de error que faciliten la auditoría de fallas. De lo contrario, los beneficios de finalidad y trazabilidad se diluyen en re-procesos manuales.

Integrar blockchain con sistemas legados exige una ingeniería de datos disciplinada, canales firmados, un modelo canónico estable y políticas documentales que preserven valor probatorio de extremo a extremo. La combinación de estos elementos permite que la inmutabilidad de la cadena multiplique —en lugar de fijar— la calidad de los registros contables públicos (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; COSO, 2013; INTOSAI, 2013; Auditoría General de la Nación, 2022; Ley 25.506, 2001).

3.5.8 Custodia de claves y gestión de identidades

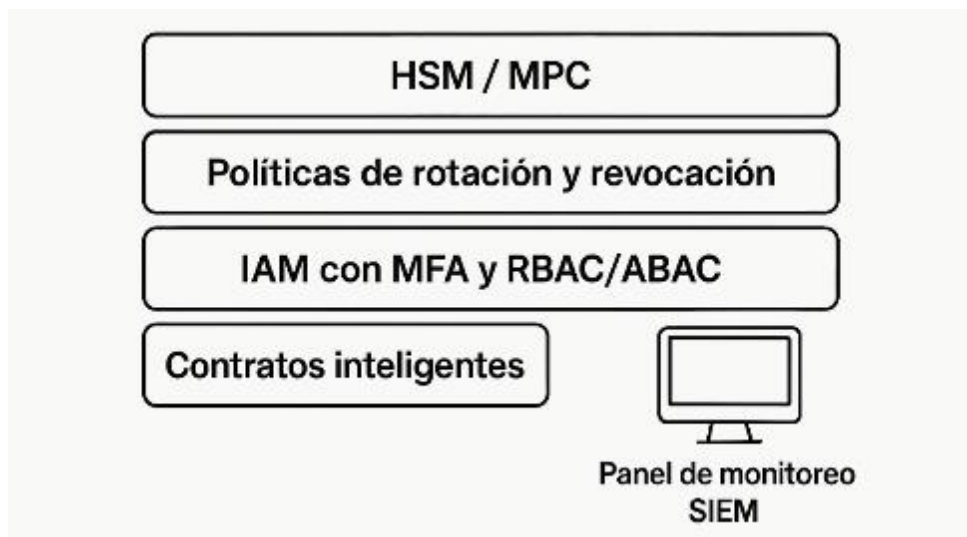
En un sistema contable basado en blockchain, las claves privadas cumplen el rol funcional de un sello de firma: habilitan o impiden asientos y aprobaciones. Su pérdida, uso indebido o robo puede originar actos inválidos o impedir operaciones legítimas. La gobernanza técnica debe, por tanto, priorizar custodia segura de claves, gestión del ciclo de vida de identidades y trazabilidad de responsabilidades (Banco Interamericano de Desarrollo [BID], 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). En auditoría del sector público, la evidencia debe ser “suficiente y apropiada” para sustentar conclusiones (INTOSAI, 2013, ISSAI 100), lo que implica que cada autorización, firma o rechazo quede asociado a una identidad verificable y a un mecanismo criptográfico confiable. Al mismo tiempo, el control interno exige “segregación de funciones” para reducir riesgos de fraude o error (COSO, 2013, secc. Componentes del control).

En práctica, conviene separar dos capas. Primero, la custodia de claves: almacenar llaves raíz y operativas en módulos de seguridad de hardware (HSM), aplicar multi-party computation (MPC) o multi-firma para aprobar operaciones sensibles, definir políticas de rotación, revocación y recuperación, y registrar todo acceso en logs inviolables. Segundo, la gestión de identidades y accesos (IAM): federar identidades con directorios institucionales, exigir autenticación multifactor (MFA), aplicar permisos mínimos necesarios (least privilege), modelos RBAC/ABAC con separación de deberes, y auditorías periódicas de altas, bajas y modificaciones (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Cuando los asientos se originan en integraciones sistema-a-sistema, los mensajes

deben firmarse (por ejemplo, JWS/JWT) y trazarse de extremo a extremo, para que la autoría técnica sea tan verificable como la humana. La Figura 38 sintetiza la gobernanza de claves e identidades, distinguiendo la capa de custodia criptográfica de la gestión de accesos e identidades operativas.

Figura 38

Gobernanza de claves e identidades



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

La normativa local otorga marco jurídico a estas prácticas. La Ley 25.506 reconoce la equivalencia funcional de la firma digital con la firma ológrafa siempre que se preserven autoría e integridad mediante procedimientos seguros y verificables (Ley 25.506, 2001). Ello refuerza la necesidad de políticas sobre quién puede firmar y con qué garantías, cómo revocar certificados comprometidos, y de qué modo evidenciar que un asiento fue autorizado por la persona y el rol correctos. INTOSAI, por su parte, vincula la calidad de la evidencia con la fiabilidad de los controles de TI, lo que en entornos distribuidos incluye el tratamiento criptográfico de identidades, llaves y trazas (INTOSAI, 2013).

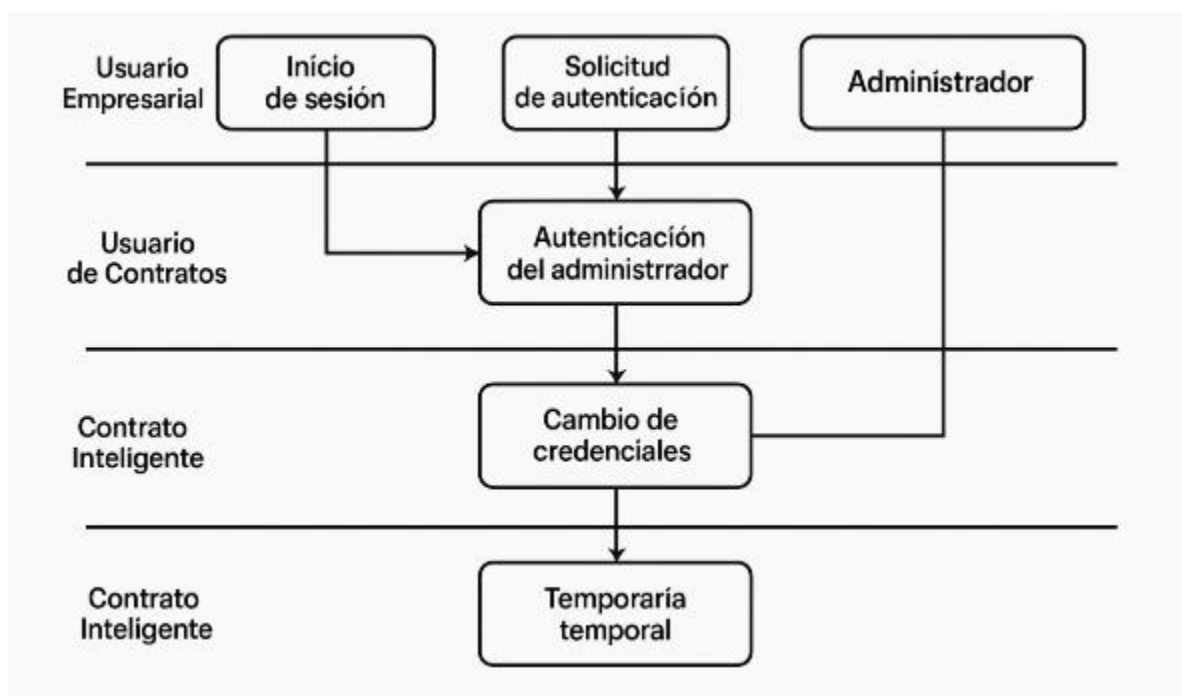
A nivel operativo, una política de claves para el consorcio (OA, AGN, SIGEN, Hacienda) debería cubrir: jerarquías de claves (raíz, emisión, operación), separación de dominios (producción/pruebas), roles custodios distintos de los roles aprobadores, inventario y clasificación de llaves, umbral de co-firmas según riesgo, rotación programada, resguardo en HSM con controles duales, procedimientos de “break-glass” para emergencias, y pruebas de restauración. En IAM, resultan críticas las políticas de password-less/MFA, la revisión trimestral de permisos, la deshabilitación automática ante rotación de cargos, y la correlación de eventos (SIEM) para alertar accesos anómalos. Estas medidas no solo reducen superficie de ataque; también

elevan la calidad probatoria de cada asiento y facilitan auditorías forenses (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

“Las credenciales y las claves son activos críticos cuya protección debe regirse por reglas explícitas de gobernanza” (BID, 2020, secc. Gobernanza de datos). A ello se suma que los proyectos deben alinearse con “objetivos públicos verificables y medibles” respecto del control de accesos y trazabilidad (BID, 2020, secc. Criterios de selección). En línea con el control interno, COSO enfatiza que la eficacia de los controles depende de una asignación clara de responsabilidades, documentación y monitoreo continuo (COSO, 2013). La Figura 39 presenta un flujo de autorización que combina autenticación multifactor y co-firma por umbral para operaciones sensibles en el sistema.

Figura 39

Flujo de autorización con MFA y co-firma por umbral



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en COSO (2013) e INTOSAI (2013).

La custodia de claves y la gestión de identidades constituyen el esqueleto de confianza del sistema: sin ellas, la inmutabilidad técnica no se traduce en responsabilidad institucional. Una arquitectura que combine HSM/MPC, MFA, RBAC/ABAC, firmas de integración y logs auditables, alineada con Ley 25.506, ISSAI 100 e ideas fuerza de COSO, permite vincular cada asiento a una persona o sistema identificable, autorizado y auditado, cerrando el círculo entre tecnología, control y validez jurídica (BID,

2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; COSO, 2013; INTOSAI, 2013; Ley 25.506, 2001).

3.5.9 Costos, capacidades y gestión del cambio

Adoptar una red de consorcio para contabilidad pública implica costos recurrentes y capacidades sostenidas: infraestructura (nube/on-premise), ciberseguridad y resguardo de claves, observabilidad y soporte 24×7, además de gobierno de datos y cumplimiento. El Banco Interamericano de Desarrollo subraya que los proyectos deben alinearse con “objetivos públicos verificables y medibles” (BID, 2020), de modo que el presupuesto y la dotación acompañen metas claras —no solo un despliegue tecnológico aislado. En paralelo, las guías del Foro Económico Mundial indican que la creación de valor exige, además de diseño técnico, “capacidades institucionales y cambios culturales” (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020), lo que sitúa a la gestión del cambio y a la formación en el centro de la implementación.

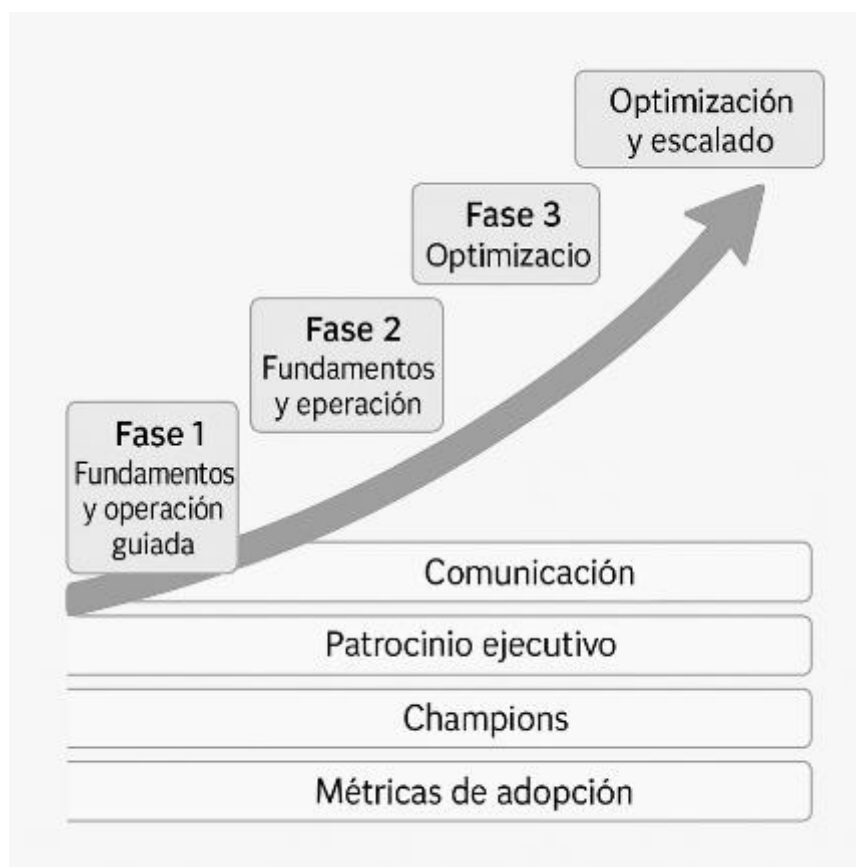
Desde una perspectiva de costos, conviene calcular el costo total de propiedad (TCO) más allá del piloto: operación coordinada de nodos, licenciamiento o soporte de plataformas, HSM/MPC para custodia de llaves, monitoreo y respuesta a incidentes, pruebas de continuidad, y auditorías periódicas sobre controles generales de TI. Cuando se trata de consorcios (p. ej., OA, AGN, SIGEN, Hacienda), el modelo de financiamiento y reparto de costos debe quedar determinado en la propia gobernanza —incluidos criterios de crecimiento y renovación tecnológica— para evitar cuellos de botella financieros (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

En cuanto a capacidades, el perfil de equipo es necesariamente mixto: contabilidad y control interno, jurídico-regulatorio, seguridad y criptografía aplicada, ingeniería de datos e integración, y administración de plataformas distribuidas. La evidencia comparada muestra que los proyectos que reservan un componente sustantivo para capacitación progresiva, manuales operativos, simulaciones de fallas y apoyo de primera línea alcanzan mejores niveles de adopción y sostenibilidad que aquellos centrados exclusivamente en el desarrollo inicial (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). En el plano metodológico, articular indicadores cuantitativos (tiempos de auditoría, tasas de conciliación, disponibilidad de la red) con evidencias cualitativas (percepción de usuarios clave, barreras organizacionales) aporta una visión integral de avance y riesgos. La Figura 40 muestra un mapa radial de capacidades y brechas, identificando los dominios críticos para sostener un proyecto de blockchain en contabilidad pública.

Figura 40*Mapa radial de capacidades y brechas*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

El control interno provee un marco para priorizar inversiones. El enfoque COSO recuerda que la eficacia de los controles se sostiene en ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y monitoreo continuo, con responsabilidades claras y documentación suficiente (COSO, 2013). INTOSAI, por su parte, demanda evidencia suficiente y apropiada para sustentar conclusiones de auditoría, lo que en entornos distribuidos supone procesos y recursos que garanticen la confiabilidad de la evidencia digital (INTOSAI, 2013). En términos prácticos, esto se traduce en presupuestar segregación de funciones, revisión periódica de accesos, pruebas de recuperación de desastres, y auditorías técnicas de contratos inteligentes, además de la gestión del cambio (comunicaciones, patrocinios ejecutivos, champions de proceso, tableros de avance). La Figura 41 presenta una curva de madurez para la gestión del cambio, que vincula fases de adopción con capacidades de control interno y auditoría.

Figura 41*Curva de madurez y gestión del cambio*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en COSO (2013) e INTOSAI (2013).

Frente al déficit de capacidades habitual en administraciones públicas, conviene planificar una curva de madurez: Fase 1 (capacitación base y operación guiada), Fase 2 (automatización de controles ex ante y tableros de auditoría), Fase 3 (optimización y escalado a otras dependencias). La estrategia se refuerza con acuerdos de colaboración interinstitucional, convenios con universidades y provisión de servicios compartidos para nodos y seguridad, reduciendo costos unitarios (BID, 2020). El éxito operacional depende de financiar el ciclo completo (TCO), desarrollar competencias transversales y gestionar el cambio como un entregable crítico, no accesorio (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; COSO, 2013; INTOSAI, 2013).

3.5.10 Marco legal, validez probatoria y responsabilidad

Asegurar la validez jurídica de los asientos en una red blockchain implica armonizar tres planos: (a) reconocimiento legal de firmas y documentos digitales, (b) admisibilidad probatoria de evidencias criptográficas y (c) reglas de responsabilidad y reversión excepcional coherentes con el derecho administrativo. En Argentina, la Ley 25.506 establece que “la firma digital tendrá la misma validez jurídica que la firma ológrafa, en los términos de esta ley” (25.506, 2001, art. 3). Sobre esa base, las transacciones firmadas digitalmente y selladas temporalmente pueden adquirir fuerza jurídica equivalente a sus pares en papel, siempre que se cumplan los requisitos de certificación, identificación del firmante y resguardo de la integridad.

Desde una perspectiva probatoria, la literatura técnica y de políticas públicas converge en que los hashes, los sellos de tiempo y las pruebas criptográficas pueden constituir evidencia suficiente y apropiada si están enmarcados por procedimientos de cadena de custodia, metadatos verificables y controles de acceso documentados (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Dicho de otro modo, la “inmutabilidad” técnica no sustituye la gestión de evidencia: la admisibilidad exige trazabilidad del origen del dato, identificación del responsable y preservación de la integridad durante todo el ciclo de vida. En el ámbito del control público, ISSAI 100 recuerda que la evidencia debe ser suficiente, apropiada y relevante para sustentar conclusiones de auditoría (INTOSAI, 2013). La Figura 42 ilustra el ciclo de vida probatorio de un documento digital, desde su generación y firma hasta el archivo y la verificación en auditoría.

Figura 42*Ciclo de vida probatorio de un documento digital*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Ley 25.506 (2001), Decreto 182/2019, INTOSAI (2013) y Banco Interamericano de Desarrollo (2020).

El marco argentino de administración financiera dispone responsabilidades claras de registro, control y documentación para los organismos del sector público nacional; por eso, al diseñar una red de consorcio (p. ej., OA, AGN, SIGEN y Hacienda) conviene traducir esas obligaciones a reglas on-chain: quién firma, con qué credenciales, bajo qué segregación de funciones, y cómo se prueban la integridad y el momento de cada asiento (Ley 24.156, 1992). Asimismo, la política de acceso a la información pública impone publicar datos y documentos con criterios de máxima transparencia, salvo las excepciones legales; esto obliga a definir qué porción va on-chain (metadatos, huellas criptográficas) y qué porción permanece off-chain (documentos completos) para compatibilizar transparencia y protección de datos personales (Ley 27.275, 2016; Ley 25.326, 2000).

La ley de firma digital equipara efectos jurídicos “en los términos de esta ley” y su decreto reglamentario precisa condiciones de infraestructura, certificadores y procedimientos (Ley 25.506, 2001; Decreto 182/2019, 2019). Ese “en los términos” remite a cumplir requisitos técnicos y organizacionales (certificados, políticas de firma, auditorías), por lo que la arquitectura blockchain debe apoyarse en PKI y en proveedores/autoridades de certificación que satisfagan las exigencias locales.

Los proyectos de cadena de bloques en el sector público deberían respaldar explícitamente la validez legal de los registros y su uso como evidencia. La tecnología debe integrarse con marcos existentes de identidad, firma electrónica y archivo, asegurando procedimientos de reversión limitada y auditada para corregir errores sin socavar la integridad del sistema (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, secc. Recomendaciones).

En materia de reversión excepcional, el diseño debe prever mecanismos para corregir errores materiales o fraudes probados, sin convertir la excepción en regla. Una gobernanza de consorcio puede declarar nulos asientos específicos mediante transacciones correctivas firmadas por autoridades competentes, acompañadas de actas y referencias cruzadas, de modo que la historia permanezca trazable (BID, 2020). En términos de responsabilidad, el enfoque COSO exige asignación clara de roles (emisor, aprobador, auditor), actividades de control y monitoreo continuo, con documentación suficiente para sostener el debido proceso (COSO, 2013).

La factibilidad legal de un libro contable distribuido en el Estado descansa en la combinación de firma digital válida, procedimientos de evidencia y custodia, y una gobernanza que concilie transparencia, protección de datos y corrección excepcional documentada. Cuando estos componentes se alinean con la Ley 25.506, la Ley 24.156, la Ley 27.275 y la Ley 25.326, la red blockchain puede producir registros con validez probatoria y responsabilidades atribuibles, aptos para auditorías internas y externas (Ley 25.506, 2001, Ley 24.156, 1992; Ley 27.275, 2016; Ley 25.326; 2000; BID, 2020; COSO, 2013; INTOSAI, 2013).

3.5.11 Conclusiones

La conveniencia de aplicar blockchain a la contabilidad pública radica en problemas de coordinación entre múltiples actores, necesidad de verificación distribuida en tiempo casi real y posibilidad de acordar reglas comunes de operación y acceso; cuando las brechas principales se ubican en la calidad de datos, la gobernanza organizacional o la capacidad normativa, la prioridad debe desplazarse primero a cerrar esas brechas y recién después a incorporar el registro distribuido (Banco Interamericano de Desarrollo [BID], 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Este balance sugiere adoptar una hoja de ruta gradual: normalizar y estandarizar datos, definir la gobernanza del consorcio (membresía, roles, mayorías), y recién entonces programar controles ex ante en contratos inteligentes y esquemas de anclaje público para auditabilidad externa (BID, 2020; COSO, 2013; INTOSAI, 2013). La

Desde una óptica operativa, las decisiones sobre finalidad, rendimiento y seguridad deben ser explícitas. En redes abiertas, la seguridad se apoya en la acumulación de confirmaciones, mientras que en consorcios permissionados la finalidad práctica es más rápida, pero descansa en identidades fuertes y reglas claras de validación (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La noción de que “Ethereum is a transaction-based state machine” (Wood, 2014, secc. 1) recuerda que cada control programado consume recursos y debe presupuestarse: límites de gas/cuotas, capacidad de cómputo y mecanismos de monitoreo para evitar cuellos de botella en cierres y conciliaciones.

Un despliegue con propósito público debería situar la tecnología dentro de un marco de datos gobernados, responsabilidades trazables y reglas de acceso y corrección excepcionales, de modo que la integridad técnica no se contraponga con la legalidad ni con los derechos de las personas; la transparencia se logra tanto con buenas reglas como con buen código (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020, secc. Recomendaciones).

En el plano profesional, la literatura contabiliza oportunidades —integridad del rastro, trazabilidad completa, automatización de controles— junto con tensiones sobre los paradigmas clásicos de evaluación de riesgos y procedimientos de auditoría. Se proyecta una adopción progresiva y no uniforme que exige nuevas competencias en contratos inteligentes, criptografía aplicada y análisis forense de cadenas para traducir evidencias técnicas en evidencia suficiente y apropiada (Morales, 2021; Santos, 2022; INTOSAI, 2013). El valor público surge cuando la solución se diseña con datos de calidad, gobernanza clara, marco legal operativo y capacidades instaladas; de lo contrario, se corre el riesgo de “tecnificar” viejos problemas sin resolverlos (BID, 2020; COSO, 2013). La Figura 44 resume visualmente el equilibrio entre beneficios esperados y riesgos asociados a la implementación de blockchain en contabilidad pública.

Figura 44

Resumen visual de beneficios vs. riesgos.



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Banco Interamericano de Desarrollo (2020).

3.6 Marco normativo en Argentina

3.6.1 Introducción

La factibilidad jurídica de incorporar blockchain en la gestión pública argentina se sustenta en un entramado normativo que, sin regularla de manera expresa, fija bases sólidas para la integridad, trazabilidad y auditabilidad del obrar estatal. En materia de transparencia y control social, la Ley 27.275 consagra que “la presente ley tiene por objeto garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública” (art. 1). Esta garantía de máxima publicidad y formatos abiertos crea condiciones propicias para soluciones de registro distribuido interoperables con portales y sistemas de datos abiertos (Ley 27.275, 2016).

La validez jurídica de documentos y firmas en entornos digitales está reconocida hace más de dos décadas: la Ley 25.506 equipara el documento electrónico y la firma digital al soporte tradicional, y el ecosistema GDE—instituido por el Decreto 561/2016 y complementado por el Decreto 1131/2016—establece repositorio único, firma digital y trazabilidad documental en toda la Administración Pública Nacional (Ley 25.506, 2001; Decreto 561/2016; Decreto 1131/2016). En este marco, “se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático...” (Ley 25.506, 2001, art. 2), lo que dota de autenticidad e integridad a cada acto administrativo firmado (Ley 25.506, 2001).

A su vez, la protección de datos personales, esencial para el diseño de cadenas de bloques con privacidad por defecto, se rige por la Ley 25.326 (Habeas Data), que tutela el tratamiento de datos en archivos públicos y privados y garantiza derechos de acceso, rectificación y supresión (Ley 25.326, 2000). Este marco exige gobernanza de datos, minimización y seguridad, compatibles con arquitecturas blockchain de propósito público que segmenten información identificatoria y evidencias criptográficas.

En compras y contrataciones, los principios que orientan la selección del co-contratante refuerzan la alineación con soluciones de registro inmutable. El Decreto 1023/2001 (Régimen General) y su reglamentación por el Decreto 1030/2016 promueven concurrencia, publicidad y trazabilidad procedimental, directrices que pueden operativizarse mediante trazas on-chain auditables (Decreto 1023/2001; Decreto 1030/2016). En palabras del artículo 3 del Decreto 1023/2001, los procesos deben regirse por:

Razonabilidad del proyecto y eficiencia...; promoción de la concurrencia...; transparencia en los procedimientos; publicidad y difusión de las actuaciones; responsabilidad de los agentes y funcionarios...; [e] igualdad de tratamiento para interesados y para oferentes. (Decreto 1023/2001, art. 3)

El marco se completa con la Ley 25.188 de Ética en la Función Pública—que establece deberes, prohibiciones e incompatibilidades aplicables a todas las personas que se desempeñan en la función pública—y con la política de gobierno abierto impulsada por el Decreto 117/2016 (Plan de Apertura de Datos), que instruyó a los organismos a publicar activos de datos y cronogramas de apertura (Ley 25.188, 1999; Decreto 117/2016). Estas normas sostienen una cultura de integridad y rendición de cuentas donde blockchain puede oficiar como capa técnica de evidencia y certificación.

Finalmente, lineamientos y experiencias recientes muestran factibilidad operativa. La iniciativa Blockchain Federal Argentina (BFA) ofrece una red multiservicio, sin necesidad de criptomoneda, ya empleada para certificar ediciones del Boletín Oficial y otros casos de uso públicos; y la Resolución 17/2022 propuso bases para un Plan Nacional de Blockchain con foco en transparencia y desburocratización (NIC Argentina, 2019; Boletín Oficial, s. f.; Resolución 17/2022). En síntesis, aunque no hay una “ley de blockchain”, el plexo vigente sobre acceso a la información, firma y documentos electrónicos, protección

de datos, ética pública, contrataciones y gobierno abierto conforma un terreno normativo apto para desplegar soluciones blockchain orientadas a prevenir la corrupción mediante evidencia verificable, trazabilidad integral y auditoría permanente. La Tabla 27 sintetiza el plexo normativo argentino relevante para proyectos de blockchain en la gestión pública y sus principales implicancias.

Tabla 27

Plexo normativo y efectos para blockchain en la gestión pública (Argentina)

Norma (año)	Objeto	Principios clave	Implicancias	Obligaciones
Ley 27.275 (2016)	Acceso y transparencia	Máxima publicidad; excepciones	Publicación con sellos de tiempo y hash	Designar responsable; responder; publicar
Decreto 117/2016	Apertura de datos	Apertura por defecto; metadatos	Catálogos; versionado; trazabilidad	Plan de apertura; cronograma
Ley 25.326 (2000)	Protección de datos	Consentimiento; derechos ARCO	Datos off chain; huellas; mecanismos ARCO	Registrar bases; seguridad; EIPD
Ley 25.506 (2001)	Firma digital válida	Integridad; no repudio; sellado	Validación; anclaje; preservación	Certificados válidos; resguardo
Decretos 561/2016 y 1131/2016	Gestión documental digital	Autenticidad; trazabilidad	Registro de eventos; hash; interoperabilidad	Uso obligatorio; archivo
Decreto 1023/2001 y 1030/2016	Contrataciones públicas	Transparencia; concurrencia	Hash de pliegos y ofertas; logs	Publicidad; cumplimiento; plataformas
Ley 25.188 (1999)	Ética pública	Conflictos; transparencia	Logs de interacciones; huellas	Códigos; declaraciones

Nota. Elaboración propia con base en Ley 27.275 (2016), Decreto 117/2016, Ley 25.326 (2000), Ley 25.506 (2001), Decretos 561/2016 y 1131/2016 (GDE), Decreto 1023/2001 y Decreto 1030/2016, Ley 25.188 (1999) y guías de la AAIP. ARCO: derechos de acceso, rectificación, cancelación y oposición; EIPD: evaluación de impacto en la protección de datos; GDE: Gestión Documental Electrónica. La interpretación de implicancias se acota a escenarios de anclaje/huellas y no sustituye asesoramiento jurídico especializado.

3.6.2 Acceso a la información pública y transparencia activa

El derecho de acceso a la información pública en Argentina se erige como presupuesto de integridad y control social: la Ley 27.275 reconoce a “toda persona” la facultad de requerir y recibir información estatal y asigna a la Agencia de Acceso a la Información Pública (AAIP) el rol de órgano garante con autonomía funcional (arts. 1 y 19). Este mandato se traduce en principios de máxima publicidad, informalismo y transparencia activa que obligan a publicar datos en formatos abiertos y a facilitar procedimientos sencillos para las solicitudes. (Ley 27.275, 2016; ver también guías oficiales de interpretación de la AAIP). La Figura 45 muestra una línea de tiempo de hitos regulatorios entre 2001 y 2025 vinculados con firma digital, gestión documental, acceso a la información y datos abiertos.

Figura 45

Línea de tiempo de hitos regulatorios (2001–2025)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Ley 25.506 (2001), Decretos 561/2016 y 1131/2016 (GDE), Ley 27.275 (2016), Decreto 117/2016 (datos abiertos), Decreto 1023/2001 y Decreto 1030/2016 (contrataciones), y lineamientos ONC. Las fechas refieren a publicación oficial o entrada en vigencia; el eje temporal es referencial. GDE: Gestión Documental Electrónica; ONC: Oficina Nacional de Contrataciones.

En 2024, el Poder Ejecutivo dictó el Decreto 780/2024, que modificó la reglamentación previa (Decreto 206/2017) e introdujo cambios procedimentales y tecnológicos en el Sistema de Transparencia y Acceso a la Información. Entre otros puntos, definió funciones de la AAIP, previó un registro para solicitudes repetidas, habilitó la remisión a contenidos ya publicados en sitios oficiales como respuesta suficiente y estableció criterios de clasificación para la tramitación. Estos ajustes pretenden uniformar circuitos administrativos y modernizar la plataforma de gestión de pedidos. (Decreto 780/2024; Decreto 206/2017).

En los considerandos de la nueva reglamentación se enfatiza la actualización tecnológica necesaria para mejorar la experiencia de los usuarios y las métricas del sistema: “resulta menester adaptar la plataforma tecnológica existente con el fin de que esta incorpore nuevas tecnologías” (Decreto 780/2024, consid.). Esta orientación oficial se alinea con la lógica de datos abiertos y con infraestructuras verificables que podrían respaldar trazabilidad y auditoría algorítmica.

Al mismo tiempo, la reforma suscitó críticas de organizaciones de la sociedad civil, que alertaron sobre riesgos de regresión en estándares de transparencia—como la ampliación de causales para denegar información o la validación amplia de respuestas meramente remisivas—y reclamaron su revisión o derogación por posible afectación del derecho. Diversas coaliciones y centros de estudio señalaron que la regulación “restringe el acceso” y podría debilitar el control ciudadano, proponiendo restablecer parámetros de máxima publicidad y proporcionalidad en las excepciones. (ACIJ, 2024; Directorio Legislativo, 2024; Rendir Cuentas, 2024).

El plexo de acceso a la información y transparencia activa habilita condiciones normativas compatibles con soluciones blockchain orientadas a prevenir la corrupción—por ejemplo, anclar evidencias de publicación, sellar tiempo de documentos y reforzar la auditabilidad de procesos—, pero la evolución reglamentaria de 2024 exige atención a su implementación para que las innovaciones tecnológicas se traduzcan efectivamente en mayor apertura y no en barreras de acceso. (Ley 27.275, 2016; Decreto 780/2024, 2024).

3.6.3 Protección de datos personales

El tratamiento de datos personales en la administración pública argentina se rige por la Ley 25.326 y su decreto reglamentario 1558/2001, que establecen principios y obligaciones aplicables a cualquier soporte o medio técnico. Entre los ejes rectores destacan licitud, finalidad, calidad, seguridad y confidencialidad, además de los derechos de acceso, rectificación, actualización y supresión (ARSU). La norma exige que los datos sean “ciertos, adecuados, pertinentes y no excesivos” respecto de la finalidad del

tratamiento y que se destruyan cuando dejen de ser necesarios para esa finalidad (arts. 4.1 y 4.7), pautas que obligan a diseños de sistemas con minimización por defecto y ciclos de vida acotados.

En el sector público, la regla general de consentimiento admite excepciones cuando el tratamiento sea necesario “para el ejercicio de funciones propias de los poderes del Estado” o por obligación legal (art. 5.2.b). Aun así, rigen los principios de finalidad, proporcionalidad y seguridad, por lo que toda recolección debe justificarse, limitarse y resguardarse con medidas técnicas y organizativas adecuadas (arts. 4, 9 y 10; Decreto 1558/2001). En términos operativos, ello se traduce en inventarios de datos, bases registradas y trazabilidad de accesos, con documentación de riesgos y salvaguardas.

Para la implantación de blockchain en trámites y servicios públicos, el encuadre legal demanda arquitectura “privacy by design”: 1) registrar on-chain solo evidencias (hashes) y metadatos estrictamente necesarios; 2) mantener los datos identificatorios off-chain bajo control del organismo; 3) aplicar seudonimización gestionada (vinculación en custodia) y, cuando corresponda, anonimización robusta; 4) habilitar rectificación/supresión actuando sobre la fuente off-chain mientras la cadena conserva únicamente pruebas de integridad; 5) evaluar permisos y segmentación por casos de uso en redes permissionadas (p. ej., BFA) para asegurar control de acceso y auditoría. La AAIP recomienda “medidas de seguridad... para el tratamiento y conservación de los datos personales” y lineamientos de responsabilidad proactiva, que resultan plenamente compatibles con este enfoque.

Además, los proyectos que impliquen tecnologías emergentes o tratamientos de alto riesgo deben realizar Evaluaciones de Impacto en la Protección de Datos (EIPD). La guía AAIP-URCDP define a la EIPD como un mecanismo preventivo que minimiza daños a la privacidad mediante identificación de riesgos y planes de mitigación desde etapas tempranas del ciclo de vida del proyecto.

Cuando nodos o proveedores de infraestructura se ubiquen fuera del país, resultan aplicables las reglas de transferencias internacionales. Argentina mantiene una decisión de adecuación de la Comisión Europea (2003/490/CE), lo que facilita flujos desde la UE; en ausencia de adecuación o ante terceros países, deben emplearse garantías contractuales y organizativas idóneas, conforme criterios de autoridades europeas y locales.

El marco vigente habilita el uso de blockchain en la gestión pública si el diseño técnico se alinea con los principios legales: minimización, finalidad específica, seguridad y gobernanza demostrable. La seudonimización y el anclaje criptográfico de evidencias, combinados con registros permissionados y EIPD, permiten compatibilizar inmutabilidad con derechos de actualización y supresión, reforzando la integridad y auditabilidad sin exponer datos personales. (Ley 25.326, 2000; Decreto 1558/2001, 2001; AAIP, 2018, 2020, 2024).

3.6.4 Documentos electrónicos, firma digital y validez probatoria

El andamiaje jurídico argentino reconoce la eficacia del documento electrónico y de las firmas electrónica y digital, y lo articula con la gestión administrativa digital. La Ley 25.506 establece el principio de equivalencia funcional y, de modo expreso, dispone: “Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital” (art. 3). Este mandato se complementa con el artículo 288 del Código Civil y Comercial, que satisface el requisito de firma en instrumentos electrónicos mediante firma digital que asegure autoría e integridad. (Ley 25.506, 2001; CCyC, art. 288).

La actualización normativa de 2018 reforzó ese marco: la Ley 27.446, en su Capítulo I (“Firma digital. Gestión documental electrónica”), modificó y derogó disposiciones de la Ley 25.506 para consolidar la infraestructura de firma y su inserción en el procedimiento administrativo digital. En 2019, el Decreto 182/2019 aprobó la reglamentación vigente de la Ley 25.506, reemplazó regulaciones anteriores y precisó procedimientos para certificadores, licenciamiento y operación de la Infraestructura de Firma Digital. (Ley 27.446, 2018; Decreto 182/2019, 2019).

En el ámbito de la Administración Pública Nacional, la validez probatoria y operativa se apoya en los sistemas GDE y TAD. El Decreto 561/2016 implantó el Sistema de Gestión Documental Electrónica como “sistema integrado” para caratulación, seguimiento y registración de actuaciones y expedientes, mientras que el Decreto 1063/2016 aprobó la Plataforma de Trámites a Distancia como “medio de interacción del ciudadano con la administración” para presentaciones, notificaciones y comunicaciones por medios electrónicos. El Decreto 1131/2016, por su parte, creó el Repositorio Único de Documentos Oficiales (RUDO) para centralizar y conservar los documentos electrónicos, asegurando integridad, accesibilidad y disponibilidad. (Decreto 561/2016; Decreto 1063/2016; Decreto 1131/2016).

Bajo este contexto, los documentos firmados digitalmente en GDE y TAD gozan de eficacia jurídica y fuerza probatoria equiparable a los instrumentos en soporte papel: el principio de equivalencia funcional (Ley 25.506 y CCyC, art. 288) satisface exigencias legales de firma, y la cadena administrativa digital con RUDO preserva condiciones de autenticidad, integridad y disponibilidad que robustecen la evidencia ante auditorías y litigios. En suma, el ecosistema normativo y tecnológico habilita expedientes íntegramente digitales, con presunciones técnicas y jurídicas compatibles con mecanismos de trazabilidad avanzada — incluida su eventual anclaje criptográfico— para fortalecer la lucha contra la corrupción. (Ley 25.506; CCyC, art. 288; Decretos 561/2016, 1063/2016 y 1131/2016; Decreto 182/2019).

3.6.5 Ética pública y prevención de la corrupción

El estándar de integridad en el sector público argentino combina deberes aplicables al funcionariado con incentivos y sanciones para las personas jurídicas que interactúan con el Estado. La Ley 25.188 fija

principios de conducta, declaraciones juradas, regulación de obsequios y gestión de conflictos de intereses, constituyendo un piso de probidad y rendición de cuentas (Ley 25.188, 1999, arts. 1, 2, 13 y 18). En palabras del propio texto, establece un “conjunto de deberes, prohibiciones e incompatibilidades” para quienes ejercen la función pública (Ley 25.188, 1999, art. 1).

De forma complementaria, la Ley 27.401 incorpora la responsabilidad penal de las personas jurídicas por delitos contra la administración pública y cohecho transnacional, previendo multas, inhabilitación para contratar e incluso disolución, junto con acuerdos de colaboración y exigencias de programas de integridad proporcionales al riesgo (Ley 27.401, 2017, arts. 7–10, 22–24). Su Decreto 277/2018 reglamenta contenidos y lineamientos, y encomienda a la Oficina Anticorrupción la emisión de guías técnicas para implementar esos programas (Decreto 277/2018, 2018, arts. 4–6).

Las Guías y Lineamientos de la Oficina Anticorrupción operacionalizan estos mandatos con componentes como código de ética, capacitación periódica, reglas para contrataciones, debida diligencia de terceros, canales de denuncia y evaluación periódica de riesgos (Oficina Anticorrupción, 2018; Oficina Anticorrupción, 2025). En paralelo, la Oficina Nacional de Contrataciones actualizó el Pliego Único de Bases y Condiciones Generales, reforzando obligaciones de transparencia y estándares de integridad para proveedores del Estado (ONC, 2024). A nivel sistémico, la Ley 24.156 consolida la arquitectura de control interno y externo —con SIGEN y AGN— que previene, detecta y corrige desvíos en el uso de recursos públicos (Ley 24.156, 1992, arts. 85–104).

Este plexo normativo resulta plenamente compatible con soluciones blockchain orientadas a la prevención de la corrupción: sellos de tiempo y anclajes criptográficos para registros de obsequios, audiencias y declaraciones de intereses; trazabilidad de hitos licitatorios y de ejecución contractual; bitácoras de acceso y actuaciones administrativas; y evidencia verificable del cumplimiento de programas de integridad en grandes contrataciones (Ley 25.188, 1999; Ley 27.401, 2017, art. 24; ONC, 2024). En síntesis, la combinación de ética pública, responsabilidad penal corporativa, lineamientos administrativos y controles institucionales configura condiciones de trazabilidad, auditabilidad y rendición de cuentas que blockchain puede fortalecer sin sustituir los controles existentes (Oficina Anticorrupción, 2018; Ley 24.156, 1992).

3.6.6 Contrataciones públicas electrónicas y trazabilidad

El Régimen de Contrataciones habilita la tramitación electrónica integral de los procedimientos y fija los principios que deben regirlos —conurrencia, publicidad, igualdad y transparencia—, creando condiciones para la trazabilidad documental y el control social (Decreto 1023/2001, 2001, art. 3; Decreto 1030/2016, 2016). En esta línea, la reglamentación específica estructura etapas, actos y soportes digitales

compatibles con expedientes íntegramente electrónicos y con la interoperabilidad de plataformas (Decreto 1030/2016, 2016).

La plataforma COMPR.AR, administrada por la Oficina Nacional de Contrataciones, constituye el medio operativo para gestionar las compras del Estado por Internet, incluyendo publicación de pliegos, recepción de ofertas, aperturas, adjudicación y notificaciones (Disposición ONC 65/2016, 2016). Como sintetiza su norma de creación, el sistema “permite efectuar la gestión de las contrataciones públicas íntegramente a través de Internet” (Disposición ONC 65/2016, 2016). Esta digitalización, articulada con el GDE y TAD, estandariza flujos, reduce discrecionalidad y deja huellas verificables en cada hito procedimental (Decreto 561/2016, 2016; Decreto 1063/2016, 2016).

Los principios rectores del régimen —“transparencia en los procedimientos” e “igualdad de tratamiento”— se vuelven operativos cuando cada acción queda fechada, firmada digitalmente y auditada, lo que robustece la publicidad activa y la posibilidad de control ex post (Decreto 1023/2001, 2001, art. 3; Ley 25.506, 2001, arts. 2–3). En términos de diseño, ello exige catálogos de actos normalizados, sellado de tiempo y conservación íntegra en repositorios oficiales que aseguren disponibilidad y autenticidad (Decreto 1131/2016, 2016).

En este marco, la inmutabilidad y el time-stamping propio de las cadenas de bloques resultan particularmente pertinentes para el ciclo de la compra pública. El anclaje criptográfico de evidencias —hash de pliegos, ofertas y actas; sellos de tiempo sobre hitos de evaluación y adjudicación; constancias de entrega y recepción— incrementa la resistencia a la manipulación y simplifica la auditoría cruzada entre sistemas (Ley 25.506, 2001; Disposición ONC 65/2016, 2016; Decreto 1030/2016, 2016). En contrataciones de alto impacto, estos mecanismos pueden complementarse con reglas de integridad y estándares del pliego único para reforzar la trazabilidad de punta a punta (ONC, 2024).

El régimen vigente ya posibilita procedimientos 100 % electrónicos con firma digital y repositorios oficiales; sobre ese piso, blockchain aporta una capa adicional de evidencia verificable que potencia la transparencia y la auditabilidad del proceso (Decreto 1023/2001, 2001; Decreto 1030/2016, 2016; Disposición ONC 65/2016, 2016). La Tabla 28 vincula los principios de la contratación electrónica con controles concretos y tipos de evidencia on/off-chain aplicables al ciclo de compras públicas.

Tabla 28*Contrataciones electrónicas: principios ↔ controles ↔ evidencias on/off-chain*

Norma (año)	Objeto	Principios clave	Implicancias técnicas	Obligaciones
Ley 27.275 (2016)	Acceso y transparencia	Máxima publicidad; excepciones	Publicación con sellos de tiempo y hash	Designar responsable; responder; publicar
Decreto 117/2016	Apertura de datos	Apertura por defecto; metadatos	Catálogos; versionado; trazabilidad	Plan de apertura; cronograma
Ley 25.326 (2000)	Protección de datos	Consentimiento; derechos ARCO	Datos off chain; huellas; mecanismos ARCO	Registrar bases; seguridad; EIPD
Ley 25.506 (2001)	Firma digital válida	Integridad; no repudio; sellado	Validación; anclaje; preservación	Certificados válidos; resguardo
Decretos 561/2016 y 1131/2016	Gestión documental digital	Autenticidad; trazabilidad	Registro de eventos; hash; interoperabilidad	Uso obligatorio; archivo
Decreto 1023/2001 y 1030/2016	Contrataciones públicas	Transparencia; concurrencia	Hash de pliegos y ofertas; logs	Publicidad; cumplimiento; plataformas
Ley 25.188 (1999)	Ética pública	Conflictos; transparencia	Logs de interacciones; huellas	Códigos; declaraciones

Nota. Elaboración propia con base en Decreto 1023/2001, Decreto 1030/2016, lineamientos ONC y Ley 27.275 (2016). Merkle proof: prueba criptográfica de inclusión; txid: identificador de transacción en el libro mayor. Los controles se ilustran a modo de referencia y deben verificarse contra políticas de cadena de custodia, segregación de funciones y reglamentos específicos de cada organismo.

3.6.7 Gobierno abierto y datos públicos reutilizables

El gobierno abierto en Argentina vincula transparencia activa, participación y reutilización de datos, con respaldo normativo en la Ley 27.275 y su reglamentación (Ley 27.275, 2016; Decreto 206/2017, 2017). En términos operativos, la política de datos abiertos exige publicar información en formatos abiertos, con metadatos estandarizados y bajo licencias que faciliten el acceso y la reutilización por parte de la ciudadanía y el sector productivo (Ley 27.275, 2016, arts. 1 y 32).

El Decreto 117/2016 instituyó el Plan de Apertura de Datos e instruyó a los organismos del Poder Ejecutivo a elaborar y presentar un plan que identifique activos de datos y su calendario de publicación (Decreto 117/2016, 2016, art. 1). En términos del propio texto, los organismos deben presentar un “Plan de Apertura de Datos... [que] deberá detallar los activos de datos... así como el cronograma de publicación”

(Decreto 117/2016, 2016). Esta obligación se ha materializado en planes publicados y catalogados en el portal nacional de datos (JGM, 2016, 2018, 2020).

Para asegurar interoperabilidad y calidad, la Administración Pública adoptó un Perfil de Aplicación Nacional de Metadatos (versión 1.2) y guías técnicas de publicación, que unifican cómo describir conjuntos y recursos en catálogos y portales (Secretaría de Gobierno de Modernización, 2018, 2019, 2020). Estas pautas—difundidas en el paquete de apertura de datos y en la sección de herramientas oficiales—alinean la documentación con estándares nacionales e internacionales y respaldan la reutilización (Secretaría de Gobierno de Modernización, 2019).

La publicación proactiva constituye un eje rector del decreto: los datos deben difundirse de manera “proactiva, completa y oportuna” y en formatos y licencias que faciliten su uso (Decreto 117/2016, 2016). Este mandato se integra con los principios de transparencia de la Ley 27.275 y con las obligaciones de los organismos de mantener catálogos actualizados y accesibles (Ley 27.275, 2016).

Sobre este piso, la interoperabilidad de portales y catálogos—apoyada en metadatos homogéneos y en plataformas como Andino—se vincula naturalmente con mecanismos de sellado de tiempo y prueba de existencia: anclar huellas criptográficas (hash) de versiones de datasets, diccionarios de datos o series temporales en cadenas públicas o permitidas permite verificar integridad, fecha de publicación y secuencia de cambios sin alterar el régimen vigente (Secretaría de Gobierno de Modernización, 2019; Decreto 117/2016, 2016). Así, la ciudadanía puede contrastar que una distribución no fue modificada después de su publicación y que las actualizaciones respetan el cronograma comprometido (Decreto 117/2016, 2016; JGM, 2016, 2018, 2020).

El Plan de Apertura de Datos y la Ley 27.275 establecen obligaciones de publicación y reutilización en formatos abiertos; las guías de metadatos y herramientas oficiales aseguran interoperabilidad; y el uso de anclajes criptográficos añade una capa de evidencia verificable que refuerza la trazabilidad y la auditoría social, sin necesidad de modificar el marco jurídico (Decreto 117/2016, 2016; Ley 27.275, 2016).

3.6.8 Lineamientos públicos sobre blockchain y experiencias locales

En 2022, la Secretaría de Innovación Pública creó el Comité Nacional de Blockchain y aprobó el Lineamiento Nacional sobre Blockchain como anexo, fijando la coordinación política y un marco de actuación para proyectos estatales (Jefatura de Gabinete de Ministros, 2022, arts. 1–2). El propio anexo declara que el documento “propone sentar las bases y líneas de acción para la implementación de un Plan Nacional de Blockchain en Argentina” (Jefatura de Gabinete de Ministros, 2022).

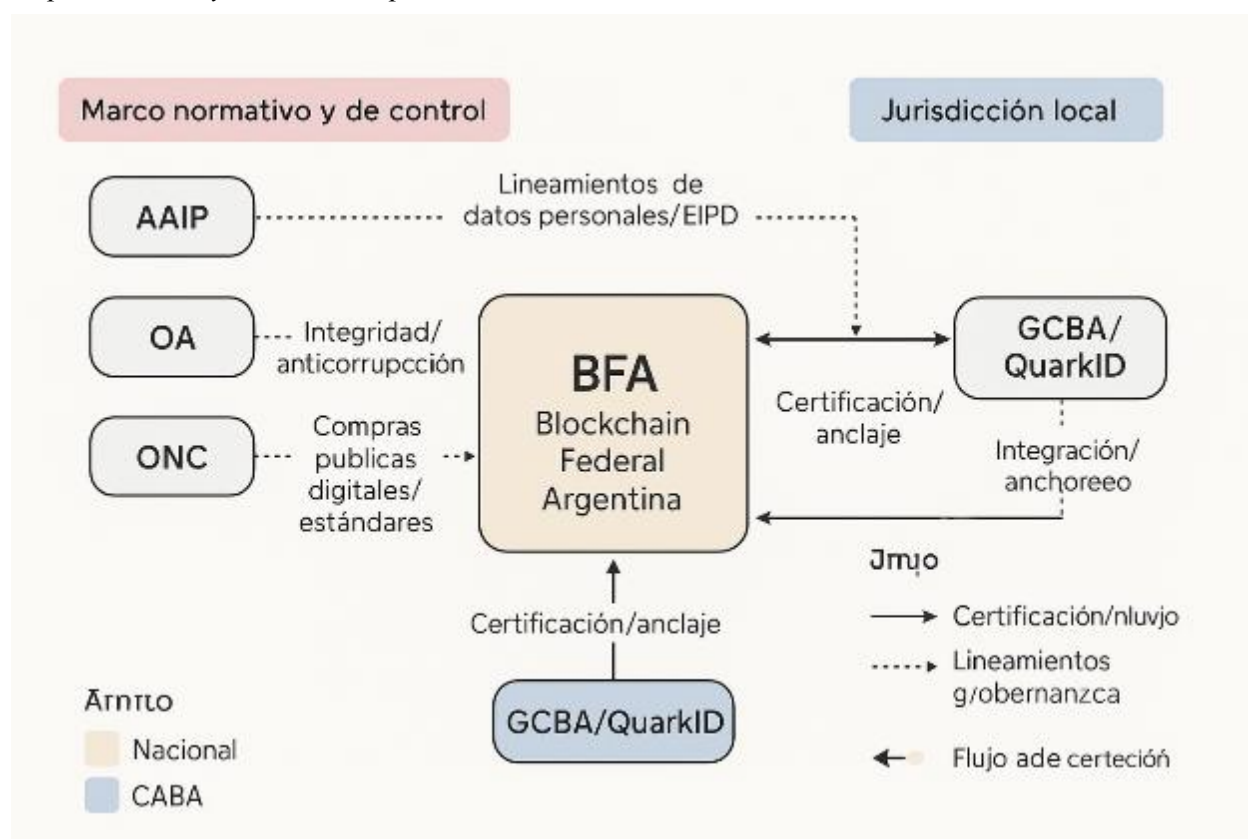
El lineamiento identifica usos públicos inmediatos vinculados con auditoría y certificación de identidad, orientados a mejorar trazabilidad, integridad y control social en procesos como licitaciones,

compras o certificaciones documentales, con foco en transparencia y desburocratización (Jefatura de Gabinete de Ministros, 2022).

En paralelo, Blockchain Federal Argentina (BFA) opera como infraestructura sin criptomoneda asociada y con costos de participación marginales para sus integrantes, diseñada para soportar servicios públicos y aplicaciones sin tarifas de transacción en cripto (BFA, s. f.-a; BFA, s. f.-b). BFA se presenta como “una plataforma multiservicios abierta y participativa” concebida para integrar desarrollos de distintos sectores (NIC Argentina, 2019). (BFA, s. f.-a; NIC Decreto 182/2019, 2019). La Figura 46 presenta un mapa de actores y lineamientos públicos relevantes para iniciativas de blockchain en la Administración Pública argentina.

Figura 46

Mapa de actores y lineamientos públicos sobre blockchain



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en fuentes normativas y lineamientos institucionales. Los nodos representan organismos y programas (p. ej., BFA, AAIP, OA, ONC, GCBA/QuarkID) y las aristas indican flujos de certificación, anclaje y gobernanza. BFA: Blockchain Federal Argentina; AAIP: Agencia de Acceso a la Información Pública; OA: Oficina Anticorrupción; GCBA: Gobierno de la Ciudad de Buenos Aires.

Las experiencias locales incluyen la certificación de ediciones del Boletín Oficial mediante sellado de tiempo y prueba de existencia, que habilitan verificación pública de integridad posterior a la publicación (Boletín Oficial de la República Argentina). Asimismo, varias implementaciones subnacionales han replicado el esquema de verificación de boletines o documentos oficiales (Municipalidad de Vicente López, 2023). En la cartera de casos de uso de BFA se encuentran además licitaciones y títulos académicos, con flujos de anclaje y consulta ciudadana. (Boletín Oficial de la República Argentina; BFA).

La política pública nacional (comité y lineamiento) y la disponibilidad de una red permissionada sin cripto como BFA conforman un andamiaje operativo para pilotos y escalamiento de soluciones blockchain en el Estado. El sellado de tiempo y el anclaje criptográfico sobre datasets, actos y expedientes refuerzan verificabilidad, trazabilidad y auditoría social, sin alterar el régimen vigente de documentación y publicidad oficial (Jefatura de Gabinete de Ministros, 2022; Boletín Oficial de la República Argentina, s. f.; BFA, s. f.).

3.6.9 Síntesis y brechas regulatorias

Argentina dispone de un andamiaje jurídico robusto para la gestión digital del Estado: equivalencia funcional de firmas y documentos electrónicos (Ley 25.506, 2001, art. 1; Ley 27.446, 2018; Decreto 182/2019, 2019), acceso a la información y transparencia activa (Ley 27.275, 2016, art. 1; Decreto 117/2016, 2016; Decreto 780/2024, 2024) e integridad/contrataciones electrónicas (Ley 25.188, 1999; Ley 27.401, 2017; Decreto 1023/2001, 2001; Decreto 1030/2016, 2016). Sobre ese piso, los lineamientos públicos de blockchain (Res. 17/2022, 2022) y la infraestructura BFA —red permissionada sin criptomoneda— permiten integrar anclajes criptográficos (hash, sellado temporal, no repudio) y registros auditables con controles de acceso y esquemas on-chain/off-chain en procesos de alto riesgo (BFA, s. f.). Como recuerda la ley de firma digital, “se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica”, base que facilita la interoperabilidad probatoria con mecanismos de anclaje (Ley 25.506, 2001, art. 1).

Aun sin ley específica de blockchain, la compatibilidad se articula por analogía con normas de documentos/firma, protección de datos y contratación (Ley 25.506, 2001; Ley 25.326, 2000; Decreto 1023/2001, 2001; Decreto 1030/2016, 2016). El principal desafío es equilibrar máxima publicidad e intimidad: transparencia y trazabilidad exigen publicación oportuna y verificable, mientras que los principios de licitud, finalidad, minimización y seguridad limitan el tratamiento de datos personales (Ley 27.275, 2016; Ley 25.326, 2000; AAIP, Res. 47/2018). Los cambios reglamentarios de 2024 sobre acceso a la información obligan a observar su implementación para evitar impactos regresivos en estándares de publicidad de actos (Decreto 780/2024, 2024). En este contexto, la EIPD como herramienta preventiva

resulta clave para diseños con blockchain que impliquen tratamientos de alto riesgo (AAIP & URCDP, 2020).

Por lo tanto, una aplicación mínimamente viable y útil deberá comprender. i) Exigir evaluaciones de impacto en privacidad (EIPD) por caso de uso, con matrices de riesgo y medidas de mitigación verificables (AAIP & URCDP, 2020). ii) Emitir guías técnicas para anclaje criptográfico y minimización: qué se registra on-chain (evidencias/huellas) y qué permanece off-chain (datos identificatorios), con sellado de tiempo y políticas de retención (AAIP, Res. 47/2018; Ley 25.506, 2001). iii) Precisar criterios de seudonimización/anonimización y el tratamiento del derecho de rectificación/supresión actuando sobre la fuente off-chain, manteniendo solo pruebas de integridad (Ley 25.326, 2000; AAIP, Res. 47/2018). iv) Alinear con buenas prácticas internacionales en gobierno digital y uso responsable de blockchain, priorizando valor público y medición de resultados (OCDE, 2019; OCDE, 2022). A nivel operativo, la obligación de planificar apertura y cronogramas de publicación respalda la trazabilidad técnica (“deberán diseñar un ‘Plan de Apertura de Datos’... con cronograma de publicación”, Decreto 117/2016, 2016), y la contratación electrónica ya prevé circuitos íntegramente digitales “como medio para efectuar en forma electrónica todos los procedimientos” (Disposición ONC 65/2016, 2016), sobre los cuales el anclaje añade evidencia verificable y auditoría continua. La Tabla 29 resume brechas regulatorias clave para proyectos de blockchain en la gestión pública y propone líneas de mitigación operativa.

Tabla 29*Síntesis de brechas regulatorias y mitigaciones*

Brecha	Impacto en el proyecto	Norma/estándar conexo	Mitigación propuesta	Estado
Ausencia de ley específica de blockchain	Incertidumbre jurídica	Leyes generales adm./civil	Políticas internas y dictámenes; sandbox regulatorio	Parcial
Datos personales en registros inmutables	Riesgo de incumplimiento ARCO	Ley 25.326 (2000)	Mantener datos off-chain; seudonimizar; EIPD	Parcial
Validez probatoria de huellas	Dudas en sede administrativa/judicial	Ley 25.506 (2001)	Cadena de custodia; sellado de tiempo cualificado; peritaje	Parcial
Interoperabilidad entre plataformas	Silos y duplicidad	Decretos GDE; estándares abiertos	APIs y esquemas comunes; hash compartidos	Pendiente
Gobernanza de redes permissionadas	Conflictos de rol y vendor lock-in	Ética pública; contrataciones	Convenio interorg.; RACI; portabilidad	Pendiente
Contratos inteligentes en compras	Falta de tipificación operativa	Régimen de contrataciones	Pilotos controlados; cláusulas de respaldo manual	Pendiente
Retención y archivo	Costos y riesgos por exceso	GDE/archivo; ISO 15489	Políticas de retención/expurgo; hash de cierre	Parcial
Soberanía tecnológica	Dependencia de nube/país	Contratos; seguridad	Requisitos de residencia de datos; cifrado extremo a extremo	Pendiente

Nota. Elaboración propia con base en Ley 25.326 (2000), Ley 25.506 (2001), Decretos GDE (2016), Decreto 1023/2001 y su reglamentación, y lineamientos de datos abiertos (Decreto 117/2016). El “estado” refleja una valoración operativa inicial (pendiente/parcial) y es ajustable según dictámenes jurídicos, auditorías y cambios normativos.

3.7 Aspectos éticos

3.7.1 Introducción

La intervención propuesta —basada en blockchain para la gestión pública— se enmarca en principios de integridad, transparencia, protección de datos personales, no discriminación, responsabilidad y rendición de cuentas, conforme estándares internacionales y normativa argentina vigente. Desde la perspectiva de integridad pública, la recomendación de la OCDE impulsa un enfoque de gobierno y sociedad en su conjunto para prevenir la corrupción y gestionar riesgos éticos en todas las fases del ciclo de políticas y servicios (OCDE, 2017; OCDE, 2020). En el plano normativo local, la ética pública exige a quienes ejercen la función pública un “conjunto de deberes, prohibiciones e incompatibilidades” que orienta la conducta y la rendición de cuentas (Ley 25.188, 1999, art. 1).

La protección de datos personales constituye un eje ineludible del diseño: los tratamientos deben ser lícitos, de finalidad determinada y proporcionales a esa finalidad, con medidas de seguridad adecuadas (Ley 25.326, 2000, arts. 4, 6 y 9; AAIP, Res. 47/2018). En términos operativos, se requiere *privacy by design* mediante minimización, seudonimización y evaluaciones de impacto en la protección de datos en proyectos de alto riesgo, especialmente cuando se integran cadenas de bloques con registros administrativos (AAIP & URCDP, 2020). Estas exigencias se articulan con marcos de gestión reconocidos internacionalmente —ISO/IEC 27001 para seguridad de la información, ISO/IEC 27701 para gestión de privacidad y ISO 37001 para sistemas de gestión antisoborno— que refuerzan controles, responsabilidades y evidencias auditables (ISO, 2022; ISO, 2019; ISO, 2025).

El proyecto debe asegurar transparencia y no discriminación sin exponer datos personales, sostener trazabilidad técnica y jurídica de las actuaciones, e incorporar mecanismos de responsabilidad y rendición de cuentas acordes con la integridad pública (OCDE, 2017; Ley 25.188, 1999; Ley 25.326, 2000). Bajo este criterio, el uso de blockchain se limita a huellas criptográficas y sellado temporal para probar integridad y secuencia de eventos, manteniendo los datos identificatorios en fuentes controladas por el organismo y sometidos a salvaguardas verificables (AAIP, Res. 47/2018; AAIP & URCDP, 2020). La Figura 47 articula principios éticos con controles técnico-organizativos y métricas indicativas para proyectos de blockchain en contabilidad pública.

Figura 47

Marco de principios éticos ↔ controles y métricas



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. El diagrama sintetiza la relación entre principios (integridad, transparencia, protección de datos, no discriminación y responsabilidad/rendición de cuentas), controles técnicos-organizativos y métricas indicativas. Sirve como guía operativa y no sustituye evaluaciones éticas específicas por proyecto.

3.7.2 Principios rectores y deberes de integridad

El marco de integridad pública exige alinear decisiones y procesos con el interés público, gestionando riesgos de corrupción y promoviendo control social colaborativo bajo un enfoque de *gobierno y sociedad en su conjunto* (OCDE, 2017; OCDE, 2020). En términos operativos, ello supone que las organizaciones públicas articulen valores, normas de conducta y mecanismos de gestión de riesgos que permeen todo el ciclo de políticas y servicios, desde el diseño hasta la evaluación, con responsabilidades claras y participación de actores internos y externos (OCDE, 2017; OCDE, 2020).

En el plano normativo argentino, la Ley 25.188 establece reglas sobre conducta, conflictos de interés, régimen de obsequios, incompatibilidades y publicidad activa, aplicables sin excepción a todo el

personal involucrado en la solución. El propio texto dispone un “conjunto de deberes, prohibiciones e incompatibilidades aplicables, sin excepción, a todas las personas que se desempeñen en la función pública” (Ley 25.188, 1999, art. 1). Estas pautas constituyen el estándar mínimo de probidad y rendición de cuentas que debe regir el diseño, la ejecución y la supervisión del proyecto. (Ley 25.188, 1999, arts. 1 y ss.).

La arquitectura ética del proyecto integra controles ex ante (p. ej., segregación de funciones, validaciones criptográficas y de cumplimiento, debida diligencia de terceros) y ex post (auditoría continua, trazabilidad de decisiones y cambios), alineados con sistemas de gestión basados en estándares internacionales. En particular, ISO 37001:2025 establece requisitos para políticas, evaluación de riesgos, controles financieros y no financieros, capacitación y mecanismos de denuncia y mejora continua, útiles para prevenir, detectar y responder al soborno en el sector público y entre contratistas (ISO, 2025; OCDE, 2020). La combinación de estos componentes refuerza la transparencia, la responsabilidad y la rendición de cuentas en cada fase del ciclo de vida de la solución.

3.7.3 Protección de datos personales y privacidad por diseño

Cuando la solución procesa datos personales, regirá el principio de licitud, lealtad y transparencia, con finalidad determinada, minimización, exactitud, plazo de conservación limitado, integridad y confidencialidad. En particular, los datos deben ser “adecuados, pertinentes y limitados a lo necesario” para los fines del tratamiento (Reglamento (UE) 2016/679, 2016, art. 5.1.c; Ley 25.326, 2000, art. 4). Estas exigencias se complementan en Argentina con el Decreto 1558/2001 —que reglamenta calidad, proporcionalidad y deber de información— y con las medidas de seguridad recomendadas por la AAIP, que orientan controles técnicos y organizativos sobre disponibilidad, integridad y acceso (Decreto 1558/2001, 2001; AAIP, Res. 47/2018).

Bajo el enfoque de privacidad desde el diseño y por defecto, la arquitectura debe: (a) mantener off-chain toda información identificatoria; (b) anclar on-chain solo evidencias criptográficas (p. ej., *hashes*, sellos temporales y referencias) necesarias para probar integridad y secuencia; (c) aplicar seudonimización gestionada y segmentación de accesos; y (d) documentar matrices de riesgo y salvaguardas a través de Evaluaciones de Impacto en la Protección de Datos (EIPD) en proyectos de alto riesgo. La guía conjunta AAIP–URCDP provee metodología práctica para identificar riesgos y medidas de mitigación, mientras que las directrices del EDPB (2025) recomiendan explícitamente privilegiar almacenamiento fuera de la cadena y referenciar datos mediante identificadores o enlaces, a fin de compatibilizar inmutabilidad con los derechos de las personas (AAIP & URCDP, 2020; EDPB, 2025). La Tabla 30 presenta una matriz ética que relaciona riesgos, controles y tipos de evidencia bajo el enfoque de privacidad desde el diseño.

Tabla 30*Matriz ética de riesgo–control–evidencia (privacy-by-design)*

Riesgo	Salvaguarda (privacy by design)	Evidencia verificable	Estándar / regla
Re-identificación	Anonimización/seudonimización robusta	Informe de k-anonymity; hash de dataset anonimizado	Ley 25.326; guías AAIP; ISO/IEC 27559
Tratamiento excesivo	Minimización de datos y fines específicos	Catálogo de datos y trazabilidad de uso	Ley 25.326; principios de finalidad
Acceso indebido	Control de acceso (RBAC/ABAC) y registro	Logs firmados; revisiones periódicas	ISO/IEC 27001/27701
Desvío de finalidad	Evaluación de compatibilidad de usos	Dictamen y registro de decisiones	Ley 25.326; AAIP
Exposición pública	Control de publicación y redaction	Acta de revisión previa; hash de versión publicada	Decreto 117/2016; datos abiertos
Trazabilidad abusiva	Pseudónimos rotativos; salting de huellas	Políticas técnicas documentadas	Buenas prácticas de seguridad
Retención indefinida	Política de retención/expurgo	Calendario de retención; acta de expurgo	GDE/archivo; ISO 15489
Falta de base legal	Identificación de bases de legitimación	Matriz de base legal por tratamiento	Ley 25.326; marco adm.

Nota. Elaboración propia con base en Ley 25.326 (2000), guías AAIP, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27559 y Decreto 117/2016. k-anonymity: métrica de anonimización;seudonimización: tratamiento que reduce identificabilidad sin eliminarla. La evidencia puede ser criptográfica (hash, sellado de tiempo) o documental (actas, registros) y debe ser auditable.

Para derechos de acceso, rectificación y supresión, el diseño debe evitar registrar datos personales inmutables en la cadena: la rectificación/supresión se ejecuta sobre la fuente off-chain, conservando en blockchain solo pruebas de integridad del documento o registro (por ejemplo, *hash* + sello de tiempo). Las directrices del EDPB subrayan que la imposibilidad técnica de borrar datos no exime del cumplimiento del RGPD; por ello, se recomiendan patrones como eliminación de claves o desvinculación de referencias cuando aplique, siempre priorizando que los datos identificatorios no ingresen on-chain (EDPB, 2025).

En términos de gobernanza y seguridad, resulta conveniente integrar un PIMS conforme ISO/IEC 27701 como extensión del ISMS definido por ISO/IEC 27001:2022, para alinear controles de privacidad y seguridad (gestión de accesos, registros de actividad, cifrado, retención y destrucción) con la

responsabilidad proactiva exigida por la AAIP (ISO, 2019; ISO, 2022; AAIP, Res. 47/2018). Esta combinación facilita auditorías, trazabilidad y rendición de cuentas sobre los tratamientos asociados a la solución.

La intervención adoptará privacidad por diseño y por defecto: datos personales off-chain, evidencias on-chain, seudonimización, controles de acceso y EIPD por caso de uso. Este esquema cumple con los principios de calidad y proporcionalidad de la Ley 25.326 y con el artículo 5 del RGPD, al tiempo que preserva verificabilidad y trazabilidad mediante *hashes* y sellos de tiempo (Ley 25.326, 2000; Reglamento (UE) 2016/679, 2016; AAIP & URCDP, 2020). La Tabla 31 ofrece un checklist de Evaluación de Impacto en la Protección de Datos (EIPD) específico para proyectos con blockchain en el sector público.

Tabla 31*Checklist EIPD para proyectos con blockchain*

Ítem de verificación	Evidencia requerida	Responsable	Frecuencia / Etapa
Finalidad específica y legítima definida	Documento de finalidad	Titular del proceso	Diseño
Base legal identificada	Matriz de base legal	Asesoría legal	Diseño
Minimización de datos aplicada	Catálogo de datos mínimo	Equipo técnico	Diseño/Construcción
Matriz de datos y flujos on/off-chain	Diagrama validado	Arquitectura	Diseño
Evaluación de Impacto (EIPD/DPIA)	Informe EIPD y riesgos	Protección de datos	Antes de pilotear
Medidas técnicas y organizativas	Inventario de controles	Seguridad de la información	Construcción
Política de retención y expurgo	Calendario aprobado	Archivo/Gestión documental	Construcción/Operación
Gestión de derechos ARCO	Procedimientos y formularios	Protección de datos	Operación
Gobernanza y RACI definidos	Matriz RACI	Proyecto/Autoridad	Diseño
Evaluación de proveedores	Contratos y DD de seguridad	Compras/Seguridad	Contratación
Cláusulas contractuales de datos	Anexos de tratamiento	Compras/Legal	Contratación
Pruebas de seguridad y logging	Informe de pruebas; txid de anclajes	Seguridad/QA	Pre-producción
Plan de respuesta a incidentes	Plan aprobado y probado	Seguridad/Operaciones	Operación
Registro de incidentes y lecciones	Libro de incidentes	Seguridad/Calidad	Continuo
Formación y concientización	Registro de capacitaciones	RR. HH./Seguridad	Periódica

Nota. Elaboración propia con base en Ley 25.326 (2000), guías AAIP y estándares ISO/IEC 27001–27701. EIPD/DPIA: evaluación de impacto en protección de datos; RACI: matriz de responsables (Responsable, Accountable, Consulted, Informed). NA: no aplica. Este checklist se archiva junto al expediente del proyecto y se actualiza por hito (diseño, construcción, pre-producción, operación).

3.7.4 Transparencia, trazabilidad y acceso a la información

La transparencia proactiva y comprensible es un eje de la intervención: se publicarán registros y métricas no sensibles en formatos abiertos, con metadatos verificables y licencias de reutilización que permitan el escrutinio y uso por terceros (organismos de control, academia y ciudadanía) sin barreras indebidas (Ley 27.275, 2016, arts. 1 y 32; Decreto 117/2016, 2016). En términos de política pública, estas obligaciones se integran con principios de integridad y rendición de cuentas que demandan información útil, oportuna y reutilizable (OCDE, 2020).

La trazabilidad inmutable que aporta blockchain funciona como capa técnica de evidencia (sellado temporal, prueba de integridad y no repudio) siempre que el diseño preserve la interpretabilidad de los datos y la explicabilidad de las reglas de negocio, de modo que la transparencia sea significativa para el control social (OCDE, 2020; Ley 25.188, 1999). En palabras de la propia normativa de acceso, la política pública busca “garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública” (Ley 27.275, 2016, art. 1).

En clave operativa, se comprometen catálogos y diccionarios de datos, versionado de conjuntos con historial de cambios, tableros de métricas con definiciones y metodología, y APIs para descarga automatizada; cada liberación de datos incorporará un anclaje criptográfico (hash) con sello de tiempo sobre el paquete publicado, manteniendo fuera de cadena cualquier información personal o sensible (Decreto 117/2016, 2016; Ley 25.326, 2000). La verificación cruzada entre el portal de datos y la traza on-chain facilitará auditoría externa y permitirá detectar modificaciones no autorizadas sin afectar derechos ni revelar atributos protegidos (Ley 27.275, 2016; Ley 25.326, 2000).

La transparencia útil combina publicación proactiva y reutilizable con trazabilidad técnica y explicabilidad: los principios normativos de acceso y ética pública se materializan en datos abiertos con garantías de integridad basadas en blockchain y salvaguardas de privacidad, habilitando control ciudadano y mejora continua de la gestión (Ley 27.275, 2016; Ley 25.188, 1999; OCDE, 2020).

3.7.5 Prevención de corrupción y soborno

La solución integrará un sistema de gestión antisoborno conforme ISO 37001:2025, articulando política, evaluación periódica de riesgos, debida diligencia de terceros, controles financieros y no financieros, capacitación, canales de denuncia, investigación y mejora continua, con responsabilidades explícitas y supervisión independiente (ISO, 2025). Este enfoque se alinea con la recomendación de la OCDE, que promueve estrategias basadas en riesgos, cultura de integridad y rendición de cuentas a lo largo de todo el ciclo de gestión (OCDE, 2017; OCDE, 2020). En términos operativos, cada riesgo ético se vinculará a controles técnicos (p. ej., segregación de funciones, registros inmutables y sellado temporal) y

organizacionales (p. ej., protocolos de conflictos de interés y due diligence), con metas, indicadores y evidencia de desempeño.

Como guía de implementación, se adoptarán los componentes clave enumerados por la norma —“Los componentes clave incluyen políticas antisoborno, procedimientos de diligencia debida, controles financieros y no financieros y programas de capacitación.” (ISO, 2025)— y se documentará una matriz de riesgos-controles que permita gobernar las acciones preventivas, detectivas y correctivas, con revisiones trimestrales y auditoría interna basada en riesgos (OCDE, 2020).

En la operación cotidiana, los registros de controles (p. ej., verificación de obsequios y hospitalidades, debida diligencia de proveedores, aprobaciones de pagos, hitos de contratación) se conservarán en repositorios oficiales y se anclarán criptográficamente (hash + sello de tiempo) para fortalecer no repudio y trazabilidad sin exponer datos personales. La auditoría continua verificará eficacia de controles y alertas tempranas (detección de patrones atípicos), mientras que la línea ética asegurará confidencialidad, seguimiento y retroalimentación a la alta dirección (OCDE, 2020; ISO, 2025). En Argentina, los programas de integridad previstos por la Ley 27.401 (arts. 22–24) y los lineamientos de la OA (Res. 27/2018) ofrecen un basamento complementario y compatible para contratistas y entes con participación estatal (Ley 27.401; OA, 2018).

Un ABMS conforme ISO 37001:2025 —integrado con una gobernanza basada en riesgos y verificación independiente—, más anclajes criptográficos de evidencia operativa, reduce oportunidades de soborno, mejora la detección y robustece la rendición de cuentas, en línea con los estándares de la OCDE y con el régimen local de programas de integridad (OCDE, 2017; OCDE, 2020; ISO, 2025).

3.7.6 Equidad, no discriminación e inclusión

La intervención se diseñará para evitar sesgos en el modelado de datos y en las reglas de validación automatizadas (umbrales, listas y criterios de alerta), con pruebas de no discriminación y procedimientos de impugnación accesibles. Ello se alinea con el enfoque de políticas públicas basadas en riesgos e inclusión promovido por la OCDE —que exige participación efectiva de partes interesadas y consideración de colectivos vulnerables— y con el mandato local de no discriminación (OCDE, 2017; OCDE, 2022; Ley 23.592, 1988). Para la accesibilidad digital, se adoptarán estándares de *diseño universal* y lenguaje claro en la administración, articulando obligaciones de accesibilidad web del sector público (Decreto 891/2017; Ley 26.653, 2010).

En términos operativos, los mecanismos de participación ciudadana incorporarán formatos abiertos, versiones legibles en lenguaje claro, alternativas *offline* y asistencia para grupos con barreras tecnológicas, de forma que la intervención no excluya a personas mayores, con discapacidad, hablantes no nativos o

residentes en zonas con baja conectividad (Decreto 891/2017; Ley 26.653, 2010). A nivel técnico, se ejecutarán pruebas ex ante y ex post de disparidad (p. ej., *disparate impact* y *equality of opportunity*), ajustes de umbrales neutrales y auditoría continua con evidencia verificable, documentando cada riesgo ético y su control asociado (OCDE, 2020; OCDE, 2022).

Como principio de accesibilidad, se observarán las WCAG: “los principios que proveen la base de la accesibilidad web” establecen contenido perceptible, operable, comprensible y robusto (W3C, 2025). Esta guía se integra con la definición legal de accesibilidad en el Estado nacional y con la obligación de adaptar portales y servicios (Ley 26.653, 2010).

Equidad e inclusión se garantizan con: (i) diseño participativo y pruebas de no discriminación; (ii) accesibilidad web y lenguaje claro en todo el ciclo de vida del servicio; (iii) canales alternativos y apoyos para no excluir a grupos vulnerables; y (iv) trazabilidad auditable de decisiones y cambios. Este enfoque satisface los principios de participación inclusiva de la OCDE, la prohibición de discriminación y las obligaciones de accesibilidad del sector público argentino (OCDE, 2017; OCDE, 2020; Ley 23.592, 1988; Ley 26.653, 2010).

3.7.7 Seguridad de la información y resiliencia

La seguridad se abordará como proceso continuo y no como estado, integrando gestión del riesgo, control interno y mejora continua sobre la base del triángulo CIA —confidencialidad, integridad y disponibilidad— y de la resiliencia operativa (ISO/IEC 27001, 2022; ISO/IEC 27002, 2022; OCDE, 2020). En términos de diseño, se aplicarán principios de mínimo privilegio, defensa en profundidad y segregación de funciones, con responsabilidades claras en toda la cadena de valor del sistema (ISO/IEC 27001, 2022).

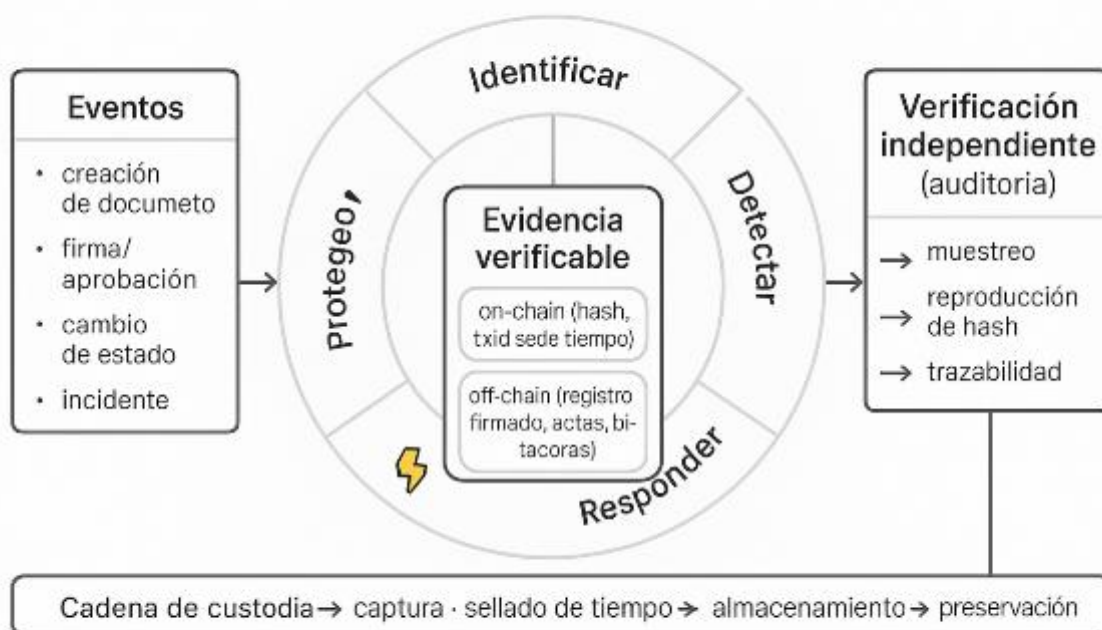
En la capa técnica, se desplegarán controles de: segmentación de redes, gestión de claves (custodia en HSM/servicios KMS, rotación, doble control), control de acceso (autenticación fuerte, privilegios mínimos, separación de ambientes), monitoreo continuo y registro, respuesta a incidentes, gestión de vulnerabilidades (análisis estático/dinámico, *hardening*), pruebas de penetración y control de cambios con trazabilidad y revisión por pares (ISO/IEC 27002, 2022; ISO/IEC 27035, 2023). En la capa de continuidad, se mantendrá un BCMS con RTO/RPO definidos, ejercicios de recuperación y dependencias críticas inventariadas (nodos validadores, clientes de consenso, oráculos, repositorios, librerías criptográficas), conforme ISO 22301 (ISO 22301, 2019).

Para el ecosistema blockchain, la arquitectura priorizará datos personales y sensibles fuera de cadena y huellas criptográficas on-chain (hash + sello temporal) para evidenciar integridad, evitando exposiciones indebidas (Ley 25.326, 2000). Se aplicarán listas de materiales de software y seguridad de la cadena de suministro para clientes/nodos (*SBOM*, firmas de versión), endurecimiento y actualización segura

de validadores, análisis de contratos inteligentes (estático, dinámico y auditoría independiente), gestión de oráculos (redundancia, reputación, *failover*) y controles de billeteras (múltiples firmas/umbrales) (ISO/IEC 27005, 2022; ENISA, 2021). La evidencia operativa (aprobaciones de cambio, despliegues, resultados de pruebas, tickets de incidente) permanecerá en repositorios oficiales y se anclará criptográficamente para reforzar no repudio sin revelar información sensible (ISO/IEC 27001, 2022). La Figura 48 muestra el ciclo de seguridad de la información y resiliencia, conectando eventos, controles y evidencias verificables en un esquema de mejora continua.

Figura 48

Seguridad de la información y resiliencia: ciclo evidencia-control-verificación



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. El ciclo muestra la relación entre eventos, controles (identificación, protección, detección, respuesta y recuperación), evidencias verificables (on/off-chain) y verificación independiente (auditoría). Incluye sellos de tiempo, registros firmados y pruebas de integridad para sustentar la cadena de custodia.

Como pauta de gobernanza, la OCDE enfatiza que la gestión de riesgos “debe integrarse en las decisiones y en el ciclo completo de las políticas y servicios”, con rendición de cuentas y controles proporcionales (OCDE, 2020). En la misma línea, se adoptará un PIMS conforme ISO/IEC 27701 como extensión del ISMS (ISO/IEC 27001), alineando privacidad y seguridad (ISO/IEC 27701, 2019).

El Marco proporciona un conjunto de actividades y resultados deseados de ciberseguridad que usan un lenguaje común y comprensible. El ‘Core’ del Marco comprende cinco funciones concurrentes y continuas —Identificar, Proteger, Detectar, Responder y Recuperar— que apoyan la gestión del riesgo y la resiliencia de las organizaciones. (NIST CSF, 2018)

La solución combinará controles técnicos verificados, resiliencia operacional probada y mejora continua: mínimos privilegios, segmentación, gestión robusta de claves, monitoreo y respuesta; continuidad y recuperación ensayadas; y un gobierno de riesgos que abarque dependencias del ecosistema blockchain (validadores, oráculos, repositorios), con evidencia anclada para auditoría sin comprometer la privacidad (ISO/IEC 27001, 2022; ISO 22301, 2019; OCDE, 2020).

3.7.8 Gobernanza ética, rendición de cuentas y participación

Se instituirá un Comité de Ética y Cumplimiento con representación técnica, jurídica, de control interno y de partes interesadas para deliberar sobre dilemas, excepciones y cambios sustantivos. Sus decisiones se documentarán, con actas, fundamentos y votos, y su trazabilidad integrará el registro auditable del proyecto, de acuerdo con los estándares de integridad pública y con el deber de probidad aplicable a toda la función pública (OCDE, 2017; Ley 25.188, 1999). En términos de gobernanza, se asignarán responsabilidades explícitas (presidencia, secretaría, oficial de cumplimiento, vocalías), reglas de recusación por conflicto de intereses y calendarios de revisión, bajo un enfoque de gestión de riesgos e involucramiento de actores (OCDE, 2017; ISO, 2021). La Figura 49 detalla una matriz RACI para la gobernanza ética y la rendición de cuentas en decisiones sensibles del proyecto.

Figura 49*Gobernanza ética y rendición de cuentas (RACI)*

	Autoridad Superior	Dueño del Dato	Protección de Datos	Seguridad de la Información	Asesoría Legal	Compras/Contrat.	Auditoría Interna	TI / Arquitectura
Publicación de datasets abiertos	A	R	C	C	C	I	I	C
Cambios de retención	A	R	C	I	C	I	C	I
Auditorías extraordinarias por riesgo	A	C	C	C	I	I	R	C
Gestión de incidentes de seguridad	A	C	C	R	C	I	C	C

	Autoridad Superior	Dueño del Dato	Protección de Datos	Seguridad de la Información	Asesoría Legal	Compras/Contrat.	Auditoría Interna	TI / Arquitectura
Intercambio de datos interorganismos	A	R	C	C	C	I	I	C
Cambios en contratos inteligentes	A	C	I	C	C	C	I	R
Acceso a datos sensibles / perfiles	A	R	C	C	C	I	I	C

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. La matriz asigna roles para decisiones sensibles (publicación de datasets, cambios de retención, auditorías extraordinarias) y vincula responsabilidades con trazabilidad de aprobaciones. RACI: Responsable (ejecuta), Accountable (aprueba), Consulted (asesora), Informed (informado).

El mandato ético se traduce en lineamientos operativos: i) control de cambios sustantivos con análisis de impacto ético y de privacidad; ii) registro de decisiones con sellado temporal y verificación de integridad; iii) seguimiento de compromisos de mejora; iv) publicación proactiva de minutas no sensibles y de indicadores de desempeño; v) protección reforzada de datos y no discriminación, con mecanismos de impugnación y reparación (Ley 25.188, 1999; OCDE, 2020). En palabras de la norma argentina, la función pública impone un “conjunto de deberes, prohibiciones e incompatibilidades aplicables, sin excepción, a todas las personas que se desempeñen en la función pública” (Ley 25.188, 1999, art. 1).

Se habilitarán canales de denuncia anónimos y protegidos, con reglas claras de confidencialidad, no represalia y trazabilidad de respuesta, y se establecerán protocolos de investigación y remediación proporcionados a la gravedad del caso. Este esquema sigue las recomendaciones internacionales de integridad basada en riesgos, reporte seguro y supervisión independiente (OCDE, 2017; OCDE, 2020; ISO, 2021).

ARTÍCULO 1º — La presente ley de ética en el ejercicio de la función pública establece un conjunto de deberes, prohibiciones e incompatibilidades aplicables, sin excepción, a todas las personas que se desempeñen en la función pública en todos sus niveles y jerarquías, en forma permanente o transitoria, por elección popular, designación directa, por concurso o por cualquier otro medio legal, extendiéndose su aplicación a todos los magistrados, funcionarios y empleados del Estado. Se entiende por función pública toda actividad temporal o permanente, remunerada u honoraria, realizada por una persona en nombre del Estado o al servicio del Estado o de sus entidades, en cualquiera de sus niveles jerárquicos. (Ley 25.188, 1999, art. 1)

Una gobernanza ética efectiva integra deliberación plural, documentación y trazabilidad de decisiones, canales de denuncia con garantías, y evaluación periódica de riesgos con controles técnicos y organizacionales, en línea con los estándares internacionales de integridad y el marco legal argentino (OCDE, 2017; OCDE, 2020; Ley 25.188, 1999; ISO, 2021).

3.7.9 Derechos de las personas y consentimiento

El consentimiento solo se empleará cuando sea idóneo y necesario; en los restantes supuestos se documentará la base jurídica correspondiente (obligación legal, ejercicio de funciones propias del Estado,

interés público) evitando cualquier forma de “consentimiento forzado”. De acuerdo con el RGPD, el consentimiento es “toda manifestación de voluntad libre, específica, informada e inequívoca” del titular, prestada mediante declaración o acción afirmativa, mientras que la Ley 25.326 exige licitud, finalidad y proporcionalidad en todo tratamiento (Reglamento [UE] 2016/679, 2016, art. 4.11; Ley 25.326, 2000, arts. 4 y 5).

Para evitar el consentimiento condicionado, se adoptarán prácticas de granularidad por finalidad, posibilidad de denegar o retirar el consentimiento sin perjuicio y separación entre lo necesario para la prestación del servicio y lo accesorio. Las directrices europeas precisan que el consentimiento no es válido si existe desequilibrio entre las partes o si se supedita a fines no necesarios; a nivel local, cuando el tratamiento sea imprescindible para funciones estatales o por obligación legal, no se requiere consentimiento, pero siguen rigiendo finalidad, minimización y seguridad (EDPB, 2020; Reglamento [UE] 2016/679, 2016, arts. 6 y 7; Ley 25.326, 2000, art. 5.2.b).

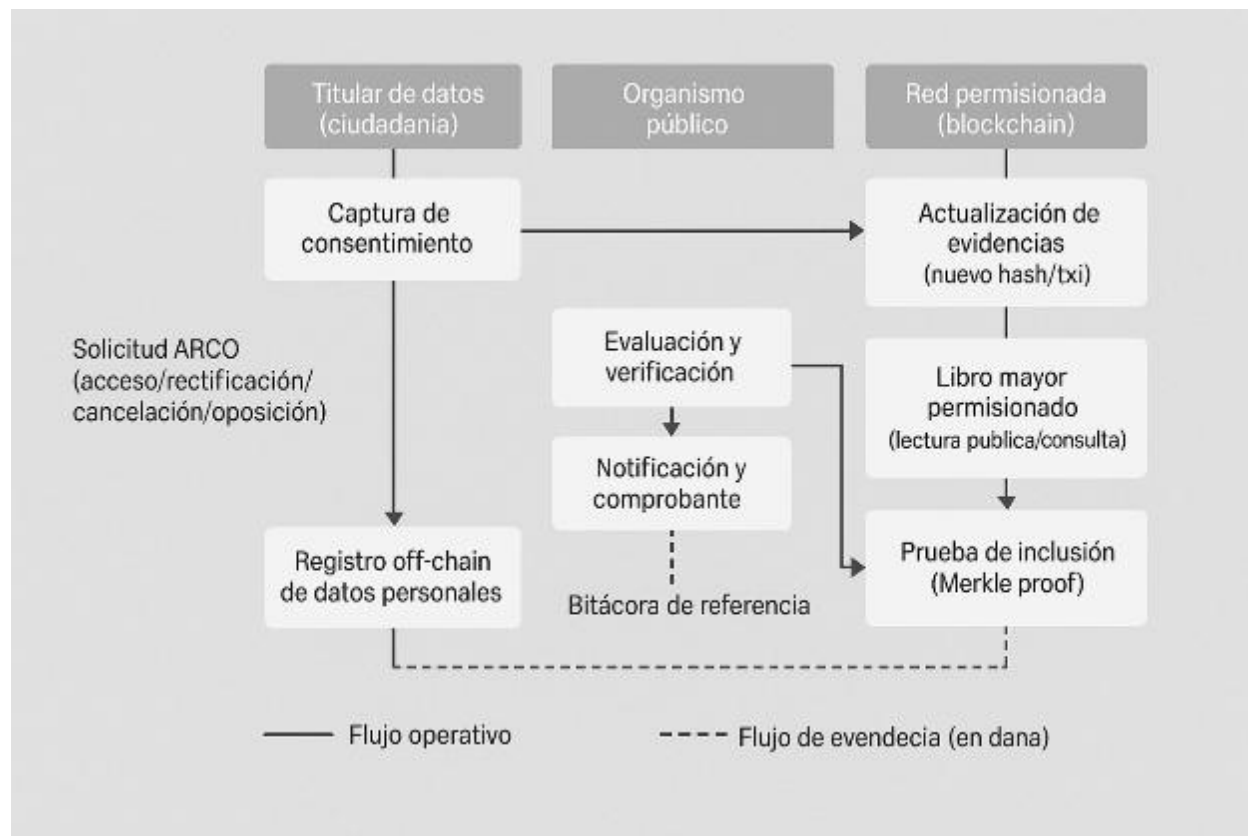
Se presume que el consentimiento no se ha dado libremente cuando el interesado no puede autorizar por separado distintas operaciones de tratamiento adecuadas en el caso concreto, o cuando la ejecución de un contrato —incluida la prestación de un servicio— se supedita al consentimiento para el tratamiento de datos personales no necesarios para dicha ejecución, o cuando existe un claro desequilibrio entre el interesado y el responsable que hace improbable que el consentimiento se otorgue libremente. (Reglamento [UE] 2016/679, 2016, consid. 43).

Para cada flujo de datos se dejará constancia de la base jurídica (p. ej., art. 5.2.b, funciones públicas; o art. 6, obligación legal/interés público), del aviso de privacidad entregado, del momento y forma de la obtención del consentimiento —si aplica—, y de los mecanismos de revocación. Se aplicará el principio de responsabilidad proactiva, con auditorías periódicas del circuito de consentimiento y evidencias verificables (Reglamento [UE] 2016/679, 2016, arts. 6 y 7; EDPB, 2020; Ley 25.326, 2000, art. 6).

Se garantizará el ejercicio de acceso, rectificación, actualización y supresión mediante procedimientos y plazos claros: el responsable deberá responder el acceso dentro de diez (10) días; y deberá rectificar, actualizar o suprimir los datos dentro de cinco (5) días hábiles de la solicitud, con canales visibles y gratuitos (Ley 25.326, 2000, arts. 14 y 16; Decreto 1558/2001, 2001). La Figura 50 representa el flujo de datos on/off-chain incorporando el consentimiento y el ejercicio de derechos ARCO sobre la fuente off-chain.

Figura 50

Flujo de datos on/off-chain con consentimiento y derechos ARCO (swimlanes)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor, utilizando el enfoque de privacy by design. Los datos personales se mantienen off-chain; en cadena sólo se registran huellas (hash, sello de tiempo, txid) y metadatos mínimos. Los eventos de acceso, rectificación, cancelación y oposición (ARCO) actúan sobre la fuente off-chain y propagan actualizaciones al registro de evidencias. ARCO: derechos de acceso, rectificación, cancelación y oposición; txid: identificador de transacción.

En blockchain, el consentimiento y los derechos se compatibilizan mediante privacidad por diseño: registrar solo evidencias (hash y sello temporal) en la cadena y mantener off-chain los datos identificatorios para permitir rectificación/supresión en la fuente; además, se asegurarán mecanismos de oposición y limitación del tratamiento cuando proceda, sin degradar el servicio esencial (Reglamento [UE] 2016/679, 2016, arts. 5 y 17; Ley 25.326, 2000, arts. 4 y 16).

El consentimiento solo se usará cuando agregue valor y sea necesario; en demás casos se adoptarán bases jurídicas objetivas y documentadas. Los derechos ARCO se garantizarán con plazos legales y canales accesibles; y, en diseños con blockchain, la preservación de datos fuera de cadena permitirá cumplir con

rectificación y supresión, mientras la cadena aportará evidencia de integridad y trazabilidad (Ley 25.326, 2000; Reglamento [UE] 2016/679, 2016; EDPB, 2020).

3.7.10 Ética de datos abiertos y publicación responsable

La publicación responsable de datos abiertos exigirá un enfoque basado en riesgos que combine legalidad, proporcionalidad y utilidad pública: se liberarán conjuntos con técnicas de anonimización acordes al riesgo de reidentificación, documentación completa (metadatos, diccionarios y versionado), licencias abiertas y advertencias sobre límites de uso, de modo que el control social sea posible sin vulnerar derechos (OCDE, 2020; Decreto 117/2016, 2016; Ley 27.275, 2016). En este marco, la transparencia proactiva se concibe como información comprensible y reutilizable, no solo como publicación formal (OCDE, 2020). La Tabla 32 resume criterios operativos para una publicación responsable de datos abiertos, equilibrando valor público y protección de derechos.

En materia de privacidad, las técnicas de desidentificación (p. ej., agregación, generalización, *k*-anonimato, *l*-diversidad, *t*-closeness y, cuando corresponda, privacidad diferencial) deberán seleccionarse según el contexto y el tipo de riesgo, con evaluación previa y pruebas de ataque razonables (ISO 20889, 2018; Grupo de Trabajo del Artículo 29, 2014). El régimen argentino agrega el estándar de calidad y proporcionalidad: los datos deben ser “ciertos, adecuados, pertinentes y no excesivos” respecto de la finalidad (Ley 25.326, 2000, art. 4), y su liberación debe preservar la imposibilidad práctica de reidentificar personas (Ley 25.326, 2000; Decreto 1558/2001, 2001).

Para asegurar calidad y trazabilidad, cada conjunto incluirá metadatos normalizados, diccionario de datos, historial de versiones y revisión de sesgos. La adopción de modelos de calidad de datos (exactitud, completitud, consistencia, actualidad, trazabilidad) y de buenas prácticas para datos en la Web facilita la reutilización y reduce ambigüedades (ISO/IEC 25012, 2008; W3C, 2017). Asimismo, cada publicación quedará respaldada con sellado temporal y anclaje criptográfico (hash del paquete liberado y del archivo de metadatos) para reforzar integridad y no repudio sin exponer información personal (Ley 27.275, 2016; Decreto 117/2016, 2016).

ARTÍCULO 1° — La presente ley tiene por objeto garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública. La información pública es toda aquella que en los términos de la presente ley generen, obtengan, transformen, controlen o custodien los sujetos obligados y que demuestre la observancia de los principios de publicidad, apertura y rendición de cuentas, sin perjuicio de los límites y excepciones que correspondan por la protección de otros derechos y bienes jurídicos. (Ley 27.275, 2016, art. 1)

Tabla 32*Ética de datos abiertos: criterios de publicación responsable*

Criterio	Regla de publicación	Control previo	Evidencia de cumplimiento	Cronograma
Minimización	Publicar solo lo necesario para el fin público	Revisión de campos sensibles	Acta de revisión	Alta
Anonimización	Aplicar técnicas adecuadas	Informe de riesgo de re-identificación	Resultado de pruebas	Alta
Granularidad	Agregar/ocultar cuando sea preciso	Evaluación de granularidad	Dictamen técnico	Alta
Formato y metadatos	Formatos abiertos + metadatos completos	Validación técnica	Ficha de metadatos	Alta
Licencia	Licencia abierta clara	Revisión legal	Licencia adjunta	Alta
Actualización	Frecuencia definida	Plan de actualización	Cronograma publicado	Periódica
Trazabilidad de cambios	Versionado e historial	Control de versiones	Hash de versiones	Continua
Evaluación de impacto	Valorar beneficios/daños	Informe de impacto	Acta de aprobación	Pre-publicación
Canal de feedback	Mecanismo para reportes	Verificación de canal	Registro de consultas	Continua
Retiro/corrección	Procedimiento claro	Revisión de solicitudes	Acta de baja/corrección	A demanda

Nota. Elaboración propia con base en Decreto 117/2016, Ley 27.275 (2016) y buenas prácticas de datos abiertos. La publicación debe equilibrar valor público y protección de derechos (riesgo de reidentificación, seguridad). Se exige versionado con historial de cambios y trazabilidad (hash de versiones) y un canal de feedback activo para retiros o correcciones.

En la práctica, cada dataset se publicará en formatos abiertos, con licencia de uso explícita, declaración de limitaciones (calidad, completitud, vigencia) y nota de responsabilidad sobre usos secundarios. Se incorporarán mecanismos de retroalimentación (issues, contacto técnico) y pruebas de no discriminación en indicadores derivados para evitar efectos adversos sobre grupos vulnerables (OCDE, 2020). La actualización seguirá un cronograma público y cada versión documentará cambios sustantivos y su justificación (Decreto 117/2016, 2016).

En cuanto a proporcionalidad, los datos deben ser “adecuados, pertinentes y no excesivos” respecto de su finalidad (Ley 25.326, 2000, art. 4).

La ética de datos abiertos exige valor público verificable y resguardo de derechos: anonimización proporcional al riesgo, documentación completa, licencias y advertencias de uso, más anclaje criptográfico y versionado. Así, la transparencia se vuelve significativa y la reutilización segura, en línea con estándares internacionales y la normativa argentina (OCDE, 2020; Ley 27.275, 2016; Ley 25.326, 2000; Decreto 117/2016, 2016).

3.7.11 Sostenibilidad e impacto ambiental

La intervención se diseñará para minimizar el consumo energético y la huella ambiental sin sacrificar seguridad ni auditabilidad. Esto implica seleccionar mecanismos de consenso y parámetros operativos eficientes (p. ej., *proof-of-stake*, límites de complejidad en contratos, políticas de *throttling*), junto con métricas verificables de desempeño energético y emisiones. La evidencia técnica muestra que el mecanismo de consenso es un determinante clave del consumo; por eso, la decisión tecnológica debe basarse en el caso de uso, el perfil de riesgo y los requerimientos de gobernanza (JRC, 2022). En paralelo, se adoptará un enfoque de gestión y reporte del desempeño ambiental alineado con buenas prácticas internacionales y con los objetivos de política pública (OCDE, 2020; Ley 27.520, 2019).

Se implementará un SGEEn conforme ISO 50001 para planificar, hacer, verificar y actuar sobre el uso energético de la solución (inventario de cargas, usos significativos, metas, medición y verificación). En la infraestructura de ejecución (centros de datos y nube) se reportarán indicadores normalizados: PUE (eficacia del uso de la energía, ISO/IEC 30134-2) y REF (factor de energía renovable, ISO/IEC 30134-3), además de un cálculo de huella de carbono del piloto con límites y supuestos explícitos. Estos elementos permitirán comparabilidad entre alternativas (on-premises vs. nube; nodos propios vs. compartidos) y toma de decisiones informada (ISO, 2018; ISO, 2016; ISO, 2016-Amd.1).

La estrategia de sostenibilidad incluirá: i) infraestructura compartida o nube con medición independiente y energía renovable documentada; ii) racionalización de nodos validadores y escalado elástico; iii) optimización criptográfica (parámetros y librerías eficientes); iv) mecanismos de apagado

programado en *testnets* y pilotos; v) plan de fin de vida y circularidad para hardware (reutilización y disposición responsable). Estas medidas se integran con un SGA tipo ISO 14001 que impulse la mejora continua del desempeño ambiental del proyecto (ISO, 2015; OCDE, 2020).

La acción climática es una obligación de política pública: la Ley 27.520 fija presupuestos mínimos para adaptación y mitigación; y la Ley 25.675 consagra principios como prevención, precaución, responsabilidad y sustentabilidad, que guían el diseño tecnológico y la contratación de infraestructura asociada (Ley 27.520, 2019; Ley 25.675, 2002). En consecuencia, la solución documentará impacto ambiental estimado del piloto y medidas de mitigación (eficiencia, energías renovables, consolidación de cargas), con revisiones periódicas y auditoría de resultados (OCDE, 2020).

La ley climática nacional establece “presupuestos mínimos de protección ambiental para garantizar acciones, instrumentos y estrategias adecuadas de adaptación y mitigación al cambio climático” (Ley 27.520, art. 1).

La interpretación y aplicación de la presente ley [...] estarán sujetas al cumplimiento de los siguientes principios: prevención (atender causas y fuentes de los problemas ambientales en forma prioritaria), precautorio (cuando haya peligro de daño grave o irreversible, la ausencia de certeza científica no debe postergar medidas eficaces), equidad intergeneracional (uso y goce apropiado del ambiente por generaciones presentes y futuras), responsabilidad (quien genera efectos degradantes afronta costos preventivos y correctivos) y sustentabilidad (gestionar el ambiente sin comprometer posibilidades de las generaciones futuras), entre otros. (Ley 25.675, 2002, art. 4).

Sostenibilidad y blockchain se articulan mediante: elección de consenso eficiente según riesgo y caso de uso; gestión energética (ISO 50001) y métricas normalizadas (PUE/REF) de infraestructura; medidas de mitigación y auditoría con mejoras continuas; y alineamiento con los principios y obligaciones ambientales vigentes. Este enfoque prioriza eficiencia, verificabilidad y transparencia del desempeño ambiental del proyecto (JRC, 2022; ISO, 2016–2022; Ley 25.675; Ley 27.520; OCDE, 2020).

En conjunto, el marco ético y normativo desarrollado en este capítulo establece las condiciones de borde de la intervención: integridad y no soborno, protección de datos y privacidad por diseño, transparencia y datos abiertos responsables, equidad e inclusión, seguridad y resiliencia, gobernanza ética y respeto por los derechos de las personas. Lejos de ser un adorno, estos principios se traducen en controles técnicos, organizacionales y documentales concretos, con evidencia verificable y trazabilidad para auditoría y control social.

Con estos requisitos éticos y jurídicos como restricción de diseño, el Capítulo 4 presenta la metodología del estudio: el enfoque mixto propuesto, el alcance y las limitaciones, las estrategias de validez y fiabilidad y el proceso de validación técnico–teórica. Esa arquitectura metodológica es la que permitirá,

más adelante, someter a prueba el diseño técnico y las métricas de desempeño de la solución basada en blockchain.

Capítulo 4: Metodología

4.1 Enfoque metodológico

Este trabajo se inscribe en un estudio de caso aplicado, con alcance descriptivo–exploratorio y diseño no experimental, orientado al diseño de una propuesta de intervención tecno–institucional en la Oficina Anticorrupción (OA). El eje está puesto en cómo debería implementarse y evaluarse una arquitectura contable basada en blockchain, más que en ejecutar un experimento ya desplegado.

El enfoque general es de métodos mixtos: se combinan componentes cualitativos y cuantitativos en un mismo programa de trabajo, articulando recolección, análisis e integración de evidencias (Creswell & Plano Clark, 2018; Tashakkori & Teddlie, 2010). En términos de diseño, se adopta un mixto de tipo convergente con integración por conexión y fusión:

Conexión: los resultados cualitativos iniciales sirven para ajustar indicadores, variables e instrumentos cuantitativos.

Fusión: en la etapa interpretativa se combinan métricas y hallazgos narrativos en matrices conjunto–tema y conclusiones integradas.

Dado que se trata de una propuesta de intervención y no de un proyecto ya implementado, la metodología opera en dos niveles complementarios:

Nivel de este Trabajo Final: revisión documental, análisis institucional y diseño del prototipo y de los indicadores de desempeño y control.

Nivel de piloto futuro: plan de medición y análisis (tablas de indicadores, plan estadístico, cadena de custodia), que queda definido como hoja de ruta replicable para la OA.

De este modo, el capítulo metodológico no sólo describe cómo se construyó la propuesta, sino también cómo debería evaluarse empíricamente si la institución decide ejecutar el piloto. La Figura 51 ofrece una vista ejecutiva del diseño mixto propuesto, destacando las fases y la integración entre componentes cuantitativos y cualitativos.

Figura 51*Mapa del diseño mixto (visión ejecutiva)*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en Creswell y Plano Clark (2018) y Tashakkori y Teddlie (2010). Véanse la Tabla 33 (Mapa del diseño mixto – conexión y fusión) y la Tabla 35 (Plan de análisis).

En línea con los criterios clásicos de metodología en las ciencias sociales, la sección precisa el tipo de diseño, las fuentes de datos, las técnicas de recolección y las estrategias de análisis, de forma esquemática pero suficiente para permitir la replicación y la evaluación del rigor (Sabino, 2014; Hernández, Fernández & Baptista, 2022). La Tabla 33 detalla el diseño mixto del estudio, indicando cómo se conectan y fusionan las fases cuantitativa y cualitativa en el tiempo.

Tabla 33*Mapa del diseño mixto (conexión y fusión)*

Objetivo	Fuente/Instr.	Unidad	Momento	Integración	Entregable
Contexto normativo/orga nizational	Revisión doc.; entrevistas	Institución/Área	Baseline	Conexión	Matriz cualitativa v1
Situación base integridad/oport unidad	ERP; event logs	Asiento/Tx	Baseline	Conexión	Dataset base + dicc.
Afinar instrumentos	Validación con participantes	Indicador	Intermedio	Conexión	Cuestionario revisado
Efectos post-intervención	ERP; anclajes; conciliación	Lote/Proceso	Post	Fusión	Matriz conjunto–tema
Adopción y barreras	Entrevistas focalizadas	Equipo/Rol	Post	Fusión	Informe de adopción
Recomendaciones	Taller; benchmark	Institución	Post	Fusión	Backlog priorizado

Nota. Elaboración propia, basada en lineamientos de integración por conexión y fusión en métodos mixtos (Creswell & Plano Clark, 2018; Tashakkori & Teddlie, 2010).

Desde la vertiente cualitativa, se plantea un estudio descriptivo–exploratorio del entorno institucional y normativo que condiciona la implementación de blockchain, con foco en factores que hoy limitan la trazabilidad contable y la transparencia en la gestión pública. Se emplearán:

Revisión documental (normativa, informes, lineamientos de control interno y auditoría).

Entrevistas semiestructuradas con informantes clave (gestión, control interno, TI) en la OA o en organismos análogos, cuando sea posible.

El análisis se organizará mediante análisis temático, buscando categorías como gobernanza, riesgos éticos, viabilidad técnica y madurez digital. Se prevé validación por participantes para reforzar credibilidad y transferibilidad de los hallazgos (Creswell & Plano Clark, 2018).

En la dimensión cuantitativa, se definen y operacionalizan indicadores para evaluar, en un eventual piloto, el impacto funcional de la solución sobre:

Eficiencia operativa: tiempos de registro, conciliación y cierre.

Integridad técnica: porcentaje de asientos con hash verificable, tasa de discrepancias on/off-chain.

Oportunidad y costo de auditoría: tiempo de auditoría por lote, costo de reproceso.

Para ese piloto se propone un diseño pre–post con línea de base, sin grupo de control, con mediciones repetidas y estimación de tamaños de efecto e intervalos de confianza. En el marco de este Trabajo Final se deja especificado el plan de análisis, aun cuando su ejecución plena dependa de la decisión institucional. La Tabla 34 presenta la operacionalización de los indicadores clave, con sus definiciones, fórmulas y fuentes de evidencia.

Tabla 34
Operacionalización de indicadores

Indicador	Definición	Fórmula	Unidad	Frecuencia	Fuente	Resp.	Umbral
Latencia publicación	$t_{\text{anclaje}} - t_{\text{registro}} (p95)$	Δt	min	Diaria	ERP + cadena	DevOps/Contab.	$p95 \leq 15$
Asientos con hash	Verificados / totales (%)	$(\#ver/\#tot) * 100$	%	Diaria	ERP + proofs	Contab.	≥ 99.5
Tiempo auditoría	Horas por lote 10k	$t_{\text{fin}} - t_{\text{ini}}$	h	Semanal	WP + ERP	Aud. Int.	≤ 8 (–20%)
Discrepancias	Divergencias por mil	$(\#disc/\#reg) * 1000$	‰	Diaria	ERP + anclajes	Ctrl. Interno	≤ 1
Excepciones contrato	Tx rechazadas (%)	$(\#exc/\#tx) * 100$	%	Diaria	Logs contrato	TI/Dev	≤ 0.5
Cobertura conciliación	Conciliados / previstos (%)	$(\#conc/\#prev) * 100$	%	Semanal	ERP + scripts	Aud. Int.	≥ 95
Costo reproceso	USD/1k registros	$\Sigma \text{costos}/(\text{reg}/1000)$	USD/1k	Mensual	Finanzas	Finanzas	–30% base

Nota. Elaboración propia. p95 = percentil 95; Δ = diferencia; pp = puntos porcentuales. La suficiencia/apropiación de evidencia y la trazabilidad se alinean con estándares de auditoría y calidad de datos (INTOSAI, 2013; ISO, 2018; ISO/IEC, 2008).

La integración se realizará por conexión (resultados cualitativos que afinan indicadores y parámetros) y por fusión (matrices que combinan números y narrativas), explicitando convergencias,

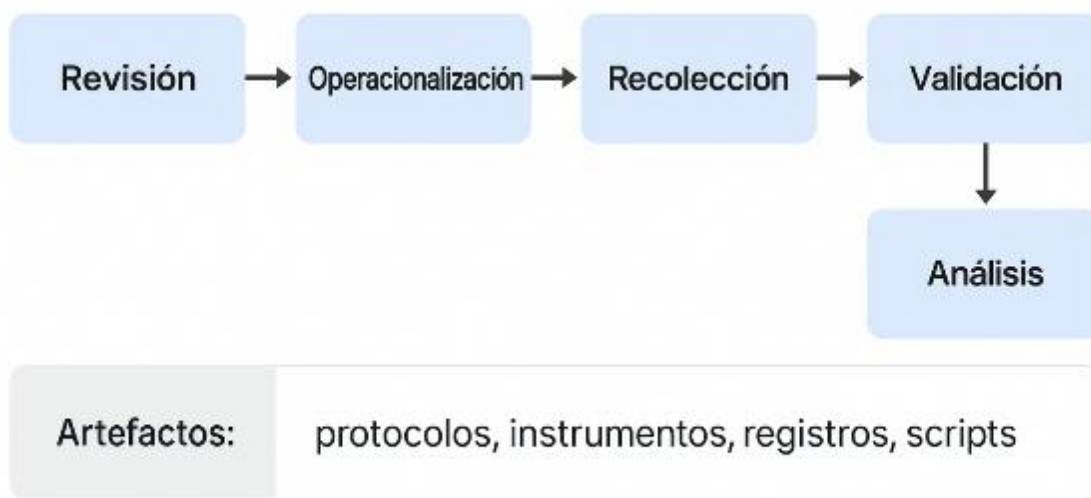
complementariedades y discrepancias. La literatura sobre gestión pública digital señala que la rendición de cuentas requiere tanto indicadores verificables como evidencia contextual sobre adopción y barreras organizacionales (OCDE, 2020). La Tabla 35 organiza el plan de análisis, relacionando cada tipo de dato con las técnicas estadísticas y cualitativas a emplear.

Tabla 35
Plan de análisis

Variable	Técnica	Software/Parám.	Supuestos	Evidencia
Latencia (min)	t/Mann–Whitney; d	Python; seed=123	Normalidad/varianzas	IC95%; d; p
Hash verificable (%)	Prop.test; IC Wilson	R; conf=0.95	n suficiente	IC95%; Δ pp; z
Tiempo aud. (h)	t pareado	Python; $\alpha=0.05$	Pareamiento	Δ medias; IC
Discrepancias (‰)	Poisson/NegBin	R (glm)	Exposición	RR; IC95%
Excepciones (%)	Chi ² /Fisher	R	Frecuencias válidas	χ^2 ; p
Costo reproceso	Medias + bootstrap	Python; 10k	Varianzas	IC95%; $\Delta\%$

Nota. Elaboración propia, basada en selección de técnicas según supuestos y en estrategias de integración cuantitativo–cualitativa (Creswell & Plano Clark, 2018; Tashakkori & Teddlie, 2010).

El método se concibe como un conjunto de procesos sistemáticos que guían la indagación y la propuesta de intervención, integrando evidencias numéricas y contextuales para comprender mejor el fenómeno (Hernández, Fernández & Baptista, 2022). La Figura 52 describe el flujo metodológico de punta a punta del estudio, representado en notación BPMN simplificada.

Figura 52*Flujo metodológico end-to-end (BPMN simple)*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en criterios de evidencia suficiente y apropiada y documentación de auditoría (INTOSAI, 2013; ISO 19011, 2018). Véanse la Tabla 34 (Operacionalización de indicadores) y la Tabla 40 (Scripts y reproducibilidad).

4.2 Alcances y limitaciones metodológicas

4.2.1 Introducción

Los alcances y limitaciones metodológicas se explicitan para orientar una lectura prudente de los resultados y de la propuesta, y para alinear el diseño con los criterios de validez, fiabilidad y rendición de cuentas propios de la gestión pública. Siguiendo la ISSAI 100, el diseño apunta a reunir evidencia suficiente y apropiada para fundamentar conclusiones útiles para la toma de decisiones (INTOSAI, 2013).

Operativamente, la circunscripción del estudio incluye: a) un caso institucional concreto (la OA), con procesos y restricciones reales; b) unidades de análisis y variables observables (asientos, lotes, procesos y actores); c) criterios de inclusión y exclusión de datos y documentos.

Estas decisiones se documentan para favorecer la replicabilidad y la trazabilidad del razonamiento analítico (ISO 19011, 2018; INTOSAI, 2013). La justificación sigue un enfoque de riesgos y control interno: los procedimientos se diseñan para reducir sesgos, explicitar supuestos y dejar constancia del juicio profesional (COSO, 2013; INTOSAI, 2013).

En este marco, el control interno se entiende como un proceso continuo realizado por la dirección y el personal de la entidad, destinado a proporcionar una seguridad razonable sobre el logro de objetivos de operaciones, información y cumplimiento, con limitaciones inherentes asociadas a errores, colusión o restricciones costo–beneficio (COSO, 2013).

En términos de validez y fiabilidad, se prevén salvaguardas específicas: Protocolos reproducibles de verificación (re-hash, pruebas de inclusión, lectura de event logs, conciliación on/off-chain); Triangulación de fuentes, instrumentos y analistas; Registros cronológicos (timestamps, bitácoras firmadas, cadena de custodia) que permitan que “otro equipo competente” replique el estudio con resultados consistentes (INTOSAI, 2013; ISO 19011, 2018). La Tabla 36 detalla el calendario y los hitos principales del trabajo de campo, indicando fechas, entregables y responsables.

Tabla 36
Calendario y hitos del trabajo de campo

Actividad	Inicio	Fin	Precondición	Entregable	Verificación
Plan de medición/muestreo	2025-10-01	2025-10-04	Indicadores aprobados	Plan v1 + hash	Manifiesto + ts
Extracción baseline + hash	2025-10-05	2025-10-06	Acceso ERP	Dataset + hashes	SHA + log
Anclaje baseline + proofs	2025-10-07	2025-10-08	Nodo operativo	Tx #B1 + proofs	TxID + bloque
Post-intervención (recolección)	2025-10-21	2025-10-28	Reglas activas	Dataset post + hash	Manifiesto post
Conciliación y análisis	2025-10-29	2025-11-04	Datasets listos	Informe concil. v1	WP-04 + hash
Reporte y devolución	2025-11-05	2025-11-09	Resultados validados	Informe final	Acta + firma

Nota. Elaboración propia, basada en planificación y gestión del programa de auditoría (ISO, 2018). Fechas en ISO 8601 (America/Argentina/Buenos_Aires). Cada hito debe generar evidencia con hash y firma.

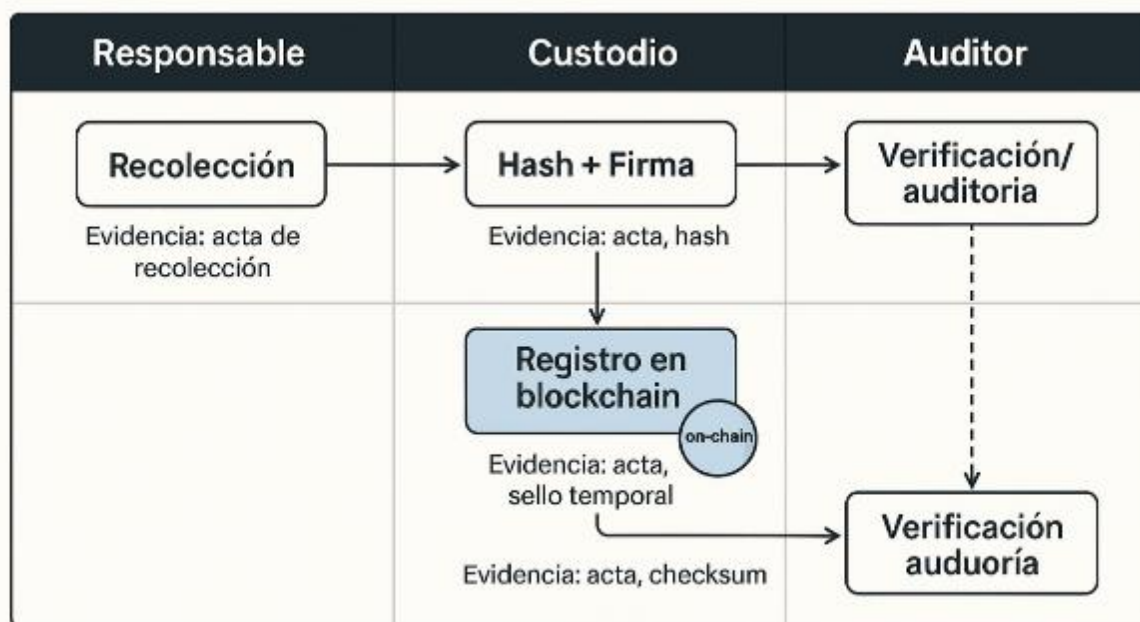
4.2.2 Alcances

El estudio se circunscribe a la OA como caso institucional y prioriza procesos contables de alto volumen y trazabilidad exigible, con el fin de valorar efectos potenciales sobre integridad, oportunidad y verificabilidad de los registros. La delimitación temporal, espacial y temática busca mantener coherencia

entre objetivos, preguntas y evidencias, definiendo con claridad unidad de análisis, fuentes y criterios de inclusión/exclusión (Hernández, Fernández & Baptista, 2022; Sabino, 2014.; Arias, 2012). La Figura 53 modela la cadena de custodia y la trazabilidad de datos mediante swimlanes, desde la generación hasta el archivo de la evidencia.

Figura 53

Cadena de custodia y trazabilidad de datos (swimlanes)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor conforme a identificación y preservación de evidencia digital y a directrices de auditoría (ISO/IEC 27037, 2012; ISO 19011, 2018).

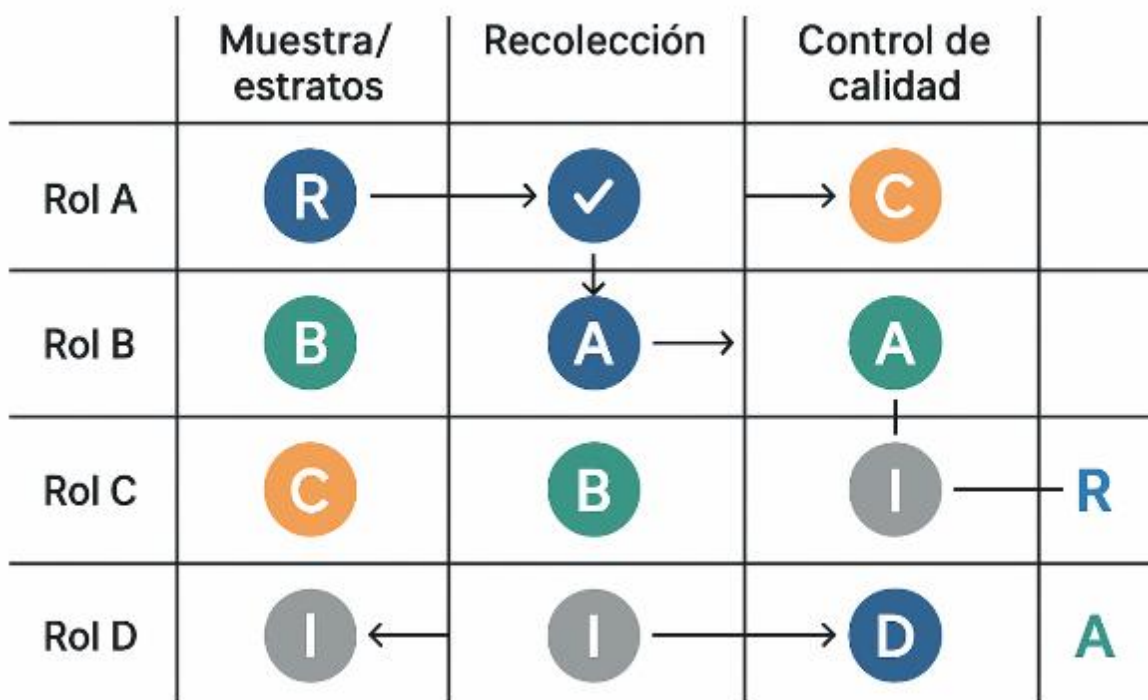
En el alcance técnico-operativo se propone incorporar controles programables (smart contracts) que codifican reglas de negocio para la aceptación y cierre de transacciones, junto con mecanismos de evidencia —hashes, pruebas de inclusión (p. ej., árboles de Merkle) y eventos sellados en el tiempo— para medir finalidad (consistencia del cierre contable) y oportunidad (tiempos entre registro y validación). Estas trazas se concilian on/off-chain mediante protocolos reproducibles de verificación y registros de auditoría, buscando evidencia suficiente y apropiada (INTOSAI, 2013; ISO 19011, 2018).

Desde el punto de vista organizacional, el alcance incluye a las áreas contables, de control interno y de tecnología de la OA. No se abordan rediseños normativos amplios, ni reformas de identidad digital, ni cambios en la estructura de clasificación presupuestaria. La selección de flujos de alto volumen y criticidad

se justifica por su impacto en la fiabilidad de la información y en la rendición de cuentas (COSO, 2013; Arias, 2012).

Como criterios prácticos de alcance se utilizarán: Periodos definidos para línea de base y medición post-intervención; Catálogos y diccionarios normalizados para los conjuntos de datos; Scripts verificables y bitácoras firmadas para la reproducción de pruebas; Resguardos de privacidad por diseño (datos identificatorios off-chain, evidencias on-chain) en armonía con el marco de protección de datos. La Figura 54 presenta un esquema RACI metodológico en swimlanes, asignando roles y responsabilidades para cada etapa del estudio.

Figura 54
RACI metodológico (swimlanes)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor en línea con segregación de funciones y monitoreo del control interno (COSO, 2013; ISO 19011, 2018).

En complemento, la Tabla 37 desglosa el RACI metodológico por actividad, precisando quién ejecuta, aprueba, asesora e informa en cada caso.

Tabla 37
RACI metodológico

Actividad	R	A	C	I	Evidencia
Definir indicadores	Contab.	Dirección	Aud. Int.	TI/Dev	Acta 01; versión
Extracción y hashing	TI/Dev	DevOps	Aud. Int.	Contab.	Log; manifiesto
Anclaje y verificación	DevOps	TI/Dev	Aud. Int.	Contab.	Tx; proofs; WP-02
Conciliación on/off	Aud. Int.	Dirección	TI/Dev	Contab.	Informe v1; WP-04
Análisis y reporte	Aud. Int.	Dirección	Contab.	TI/Dev	Informe final

Nota. Elaboración propia, basada en asignación de responsabilidades en control interno y sistemas de cumplimiento (COSO, 2013; ISO, 2021).

Finalmente, el alcance queda definido por: a) caso OA; b) procesos contables de alto volumen; c) adopción de controles programables y mecanismos criptográficos para medir finalidad y oportunidad; y d) criterios explícitos de inclusión/exclusión y documentación para asegurar validez, fiabilidad y replicabilidad (INTOSAI, 2013; COSO, 2013; Hernández, Fernández & Baptista, 2022).

4.2.3 Limitaciones

Se reconocen tres grupos principales de limitaciones:

Calidad de datos. La inmutabilidad de la cadena congela tanto aciertos como errores. Si los catálogos y diccionarios no están normalizados, las incoherencias se perpetúan y encarecen su corrección. Bajo el modelo de calidad de datos, atributos como exactitud, consistencia, completitud y trazabilidad condicionan la validez de los análisis (ISO/IEC 25012, 2008; W3C, 2017). Esto obliga a diseñar controles preventivos (validaciones, reglas de negocio, catálogos maestros) y detectivos (conciliaciones on/off-chain, re-hash, pruebas de inclusión) para sustentar evidencia suficiente y apropiada (INTOSAI, 2013).

Capacidades y gobernanza. La ausencia de comités y de una matriz RACI clara ralentiza decisiones y difumina responsabilidades. Los marcos de control interno y compliance exigen establecer

autoridades, líneas de reporte y criterios de recusación por conflicto de interés (COSO, 2013; ISO 37301, 2021). Metodológicamente, una gobernanza insuficiente introduce sesgos de ejecución (desvíos de alcance, cambios no documentados), que se mitigan con planes de proyecto, actas y trazabilidad de cambios (ISO 19011, 2018).

Costos de operación (TCO). El valor de la intervención depende de financiar todo el ciclo de vida: custodia y rotación de claves, observabilidad (registros, métricas, alertas), pruebas de penetración y auditorías periódicas, respaldo y continuidad, y actualización segura de validadores y clientes (ISO/IEC 27001, 2022; ISO/IEC 27002, 2022). Si el presupuesto se limita al despliegue inicial, aumentan los riesgos residuales y se degrada la “seguridad razonable” esperada del sistema (COSO, 2013).

Estas limitaciones son previsibles y gestionables: la normalización de catálogos y pruebas de validación mejoran la calidad de los datos; una gobernanza con RACI y supervisión independiente reduce ambigüedades decisorias; y un presupuesto que contemple CAPEX + OPEX preserva la eficacia de los controles (ISO/IEC 25012, 2008; ISO 37301, 2021; ISO/IEC 27001, 2022; COSO, 2013; INTOSAI, 2013; ISO 19011, 2018).

4.2.4 Sesgos y validez

La estrategia metodológica incorpora salvaguardas para validez interna y validez externa, y controles frente a sesgos de selección, medición y confirmación. La validez interna se vincula con atribuir correctamente los efectos a la intervención (y no a factores extraños); la validez externa, con la posibilidad de generalizar o transferir resultados a contextos afines, siempre que se documenten supuestos y condiciones de frontera (Hernández, Fernández & Baptista, 2022).

Validez interna (protocolos reproducibles). Para reducir amenazas clásicas (historia, instrumentación, sesgos del observador), se utilizarán procedimientos verificables: re-hash de documentos y asientos, pruebas de inclusión en árboles de Merkle, lectura de event logs con sello temporal y conciliación on/off-chain. Todo se documentará en guías y scripts versionados, con registros cronológicos firmados y cadena de custodia, de forma que un equipo independiente pueda replicar los resultados (INTOSAI, 2013; ISO 19011, 2018). Se prevé doble verificación de cálculos y revisiones ciegas de muestras para mitigar sesgos de confirmación (Hernández, Fernández & Baptista, 2022).

Validez externa (transferencia y límites). Se proporcionará una descripción densa del contexto (organización, procesos, datos, marco normativo), de los criterios de inclusión/exclusión y de los parámetros de configuración de la solución (red, nodos, reglas). La triangulación de fuentes (documental, trazas técnicas y entrevistas) y de analistas reduce sesgos de medición y eleva la credibilidad de los

hallazgos (INTOSAI, 2013; Creswell & Plano Clark, 2018). La Tabla 38 identifica riesgos de validez del estudio y las salvaguardas previstas para mitigarlos, en línea con la literatura metodológica y de auditoría.

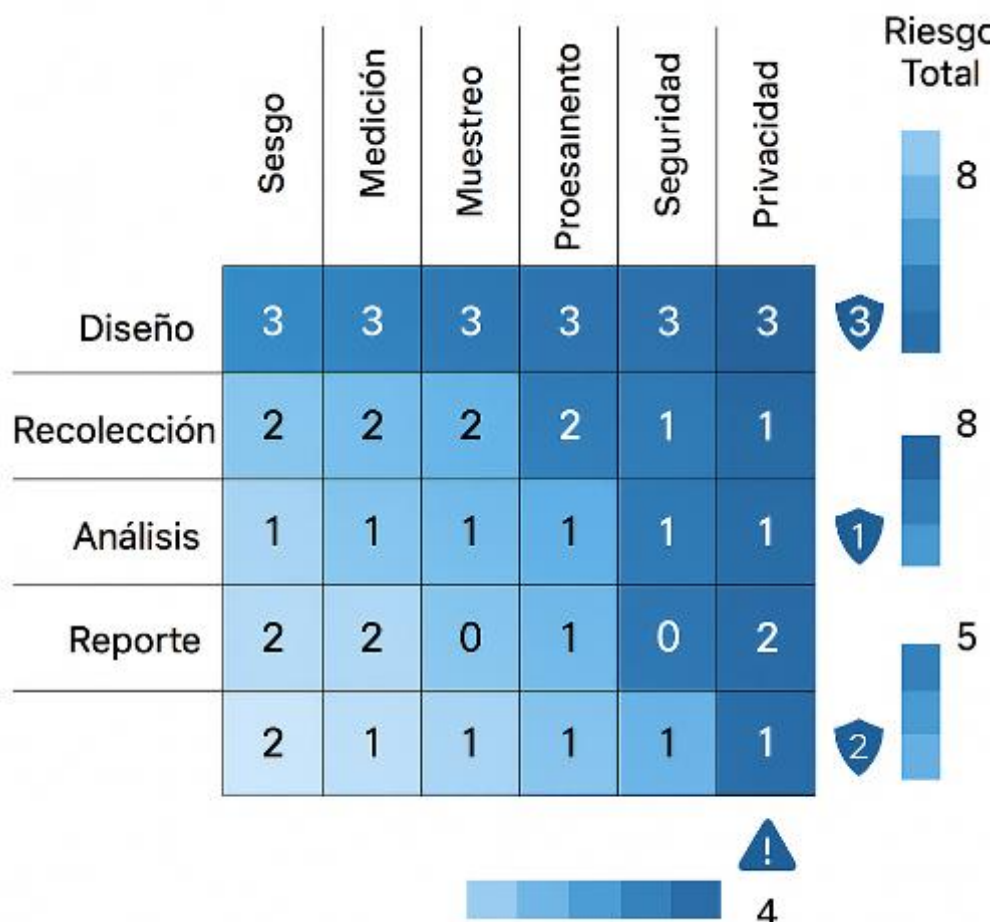
Tabla 38

Riesgos de validez y salvaguardas

Amenaza	Efecto	Salvaguarda	Evidencia
Historia	Atribución espuria	Baseline + calendario	Actas/hitos
Instrumentación	Medición inconsistente	Scripts versionados	Commits + hashes
Sesgo observador	Confirmación	Doble verificación ciega	Planillas firmadas
Maduración	Mejora por aprendizaje	Ventanas equivalentes	Cronograma
Selección	Muestra sesgada	Estratificación + aleatorio	Plan de muestreo

Nota. Elaboración propia, basada en amenazas a la validez (historia, instrumentación, sesgos, selección) y en el criterio de “evidencia suficiente y apropiada” en auditoría pública (INTOSAI, 2013; Hernández, Fernández & Baptista, 2022).

La Figura 55 representa gráficamente, mediante un mapa de calor, los riesgos de validez y fiabilidad identificados y su criticidad relativa.

Figura 55*Mapa de riesgos de validez y fiabilidad (heatmap)*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en tipologías de amenazas a la validez y en el criterio de evidencia suficiente y apropiada (INTOSAI, 2013; Hernández, Fernández & Baptista, 2022).

4.2.5 Fiabilidad

La fiabilidad se asegura mediante procedimientos reproducibles y trazables que permitan a otro profesional competente repetir los pasos y obtener resultados consistentes, coherentes con el criterio de evidencia suficiente y apropiada (INTOSAI, 2013). Se prevén: Scripts verificables y versionados (con parámetros y semillas fijadas); Sellos de tiempo sincronizados y zona horaria explícita; Bitácoras firmadas digitalmente y cadena de custodia documentada (ISO 19011, 2018; ISO/IEC 27037, 2012); Controles cruzados (re-hash, pruebas de inclusión, lectura de event logs) y doble verificación de cálculos (Hernández,

Fernández & Baptista, 2022). La Tabla 39 detalla el protocolo de recolección de datos y la cadena de custodia asociada, asegurando trazabilidad y preservación de la evidencia.

Tabla 39

Protocolo de recolección y cadena de custodia

Actividad	Evidencia	Hash	Timestamp	Repositorio	Firma/Resp.
Extracción baseline ERP	CSV v1 (10k)	sha256:...	2025-10-01 09:00–03:00	Repo /datasets	F. Pérez
Hashing de insumos	manifest.json	sha256:...	2025-10-01 09:15–03:00	Repo /hashes	L. Gómez
Publicación anclaje	Bloque #B1	tx:...	2025-10-01 09:30–03:00	Cadena perm.	J. Ruiz
Verificación Merkle	Proofs por lote	sha256:...	2025-10-01 10:00–03:00	Repo /proofs	M. Díaz
Conciliación on/off	Reporte v1	sha256:...	2025-10-01 11:00–03:00	WP /concil.	M. Díaz

Nota. Elaboración propia, basada en directrices para identificación y preservación de evidencia digital y para documentación de auditorías (ISO/IEC 27037, 2012; ISO 19011, 2018).

La Tabla 40 sintetiza los scripts utilizados y los mecanismos previstos para garantizar la reproducibilidad de los análisis.

La fiabilidad se apoya, por tanto, en automatización verificable, trazabilidad temporal y autoral, custodia formal de la evidencia y documentación exhaustiva que habilite la réplica.

Tabla 40
Scripts y reproducibilidad

Script	Versión	Parámetros	Hash script	Resultado	Revisor
extract_erp.py	a1c9f2	seed=123; chunk=5k	sha256:...	CSV base 10k	M. Díaz
rehash_manifest.py	b7e43d	algo=sha256	sha256:...	manifest.json + CSV	L. Gómez
anchor_tx.ipynb	c92d11	net=perm; gas=auto	sha256:...	Tx #B1; raíz merkle	J. Ruiz
proof_merkle.py	d0a77f	fanout=16	sha256:...	proofs.json	J. Ruiz
conciliacion.ipynb	e51b0a	threshold=5s	sha256:...	reporte_concil_v1.pdf	M. Díaz

Nota. Elaboración propia, basada en gestión de seguridad de la información, evidencia digital y documentación de auditoría (ISO/IEC 27001, 2022; ISO/IEC 27037, 2012; ISO 19011, 2018). “Versión/Commit” = identificador en control de versiones; “Hash del script” = archivo efectivamente ejecutado.

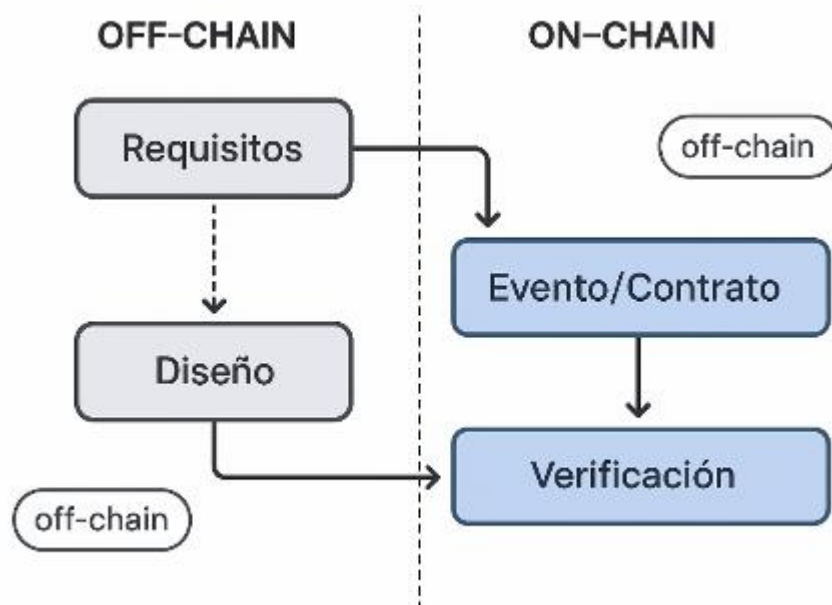
4.3 Proceso de validación técnica y teórica

La validación se estructura en dos planos complementarios: A) Técnico–funcional: demostrar que los controles y las evidencias operan como fueron diseñados. B) Teórico–normativo: corroborar que los resultados producidos son suficientes y apropiados para fines de auditoría y rendición de cuentas, según estándares como ISSAI 100 y COSO (INTOSAI, 2013; COSO, 2013).

El ciclo crear/firmar → validar/publicar → consensuar/replicar debe producir un historial verificable apto para procesos contables que exigen integridad, finalidad y trazabilidad (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Figura 56 representa, mediante un grafo, la trazabilidad on/off-chain del piloto metodológico, conectando fuentes, evidencias y verificaciones.

Figura 56

Trazabilidad on/off-chain del piloto metodológico (grafo)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor.

A) Validación técnico–funcional

1. Pruebas unitarias e integración de contratos.
Se validarán reglas de autorización, umbrales y eventos de negocio mediante casos positivos y negativos, verificando que los contratos implementen correctamente controles ex ante y dejen trazas auditables ex post (ISO 19011, 2018).
2. Verificación de evidencias en muestra estratificada.
Sobre una muestra estratificada de operaciones se ejecutará:
 - a) re-cálculo de hash y comparación con el valor publicado on-chain;
 - b) prueba de inclusión (árbol de Merkle) hasta la raíz y el bloque de referencia;
 - c) lectura y reconstrucción de event logs con sello de tiempo;
 - d) conciliación on/off-chain (ERP vs. metadatos en la cadena).

La Tabla 41 presenta el esquema de muestreo y estratificación empleado para la verificación, indicando poblaciones, tamaños muestrales y criterios de selección.

Tabla 41
Muestreo y estratificación para verificación

Estrato	N	n	Criterio inclusión	Riesgo	Justificación
Presupuesto/compr omiso	120000	384	Registros > USD 5k; top 5 áreas	Alta	Materialidad 80/20
Devengado/pago	250000	400	Pagos > USD 3k; sist. 1:k	Media	Riesgo + volumen
Contrataciones	18000	260	Hitos; cambios	Alta	Impacto reputacional
Otras operaciones	50000	200	Aleatorio simple	Baja	Cobertura residual

Nota. Elaboración propia, basada en criterios de muestreo en diseños mixtos y en textos metodológicos en español. N = población del estrato; n = tamaño muestral (Creswell & Plano Clark, 2018; Hernández, Fernández & Baptista, 2022).

La Tabla 42 detalla la trazabilidad on/off-chain del piloto metodológico, vinculando evidencias criptográficas con sus originales bajo custodia.

Tabla 42
Trazabilidad on/off-chain del piloto metodológico

Registro	Metadatos mínimos	Hash publicado	Prueba inclusión	Ubicación	Custodia
Asientos	ID, fecha, monto, área	hash:...	Proof OK	ERP/SharePoint	Contab.
Comprobantes	ID, emisor, fecha, total	hash:...	Proof OK	Repo evidencias	Ctrl. Interno
Eventos contrato	txid, bloque, tópico, ts	hash:...	Proof OK	Nodo verificador	DevOps
Bitácoras aud.	ID WP, autor, fecha	hash:...	N/A	Working papers	Aud. Int.

Nota. Elaboración propia, basada en verificación por pruebas de inclusión contra raíz de Merkle y bloque/estado de referencia; originales off-chain bajo custodia definida (Nakamoto, 2008; Wood, 2014).

3. Métricas operativas y criterios de aceptación.

La Tabla 43 fija los criterios de aceptación para cada métrica, incluyendo umbrales, tolerancias y parámetros estadísticos de evaluación.

Tabla 43
Criterios de aceptación por métrica

Métrica	Umbral p95	Tolerancia	Acción ante desvío	Resp.
Latencia (min)	≤ 15	± 2	Ajuste colas / validadores	DevOps
Hash verificable (%)	≥ 99.5	-0.2 pp	Reprocesar lote + incidente	Contab.
Tiempo auditoría (h)	≤ 8 (-20%)	± 1	Optimizar scripts/muestreo	Aud. Int.
Discrepancias (‰)	≤ 1	± 0.3	Investigación + corrección	Ctrl. Interno
Excepciones (%)	≤ 0.5	± 0.1 pp	Revisar reglas/datos	TI/Dev
Cobertura concil. (%)	≥ 95	-1 pp	Completar concil. + doc.	Aud. Int.
Costo reproceso (USD/1k)	-30% base	$\pm 5\%$	Mejoras lean + auto.	Finanzas

Nota. Elaboración propia. “Tolerancia” = banda operativa alrededor del umbral; reportar p50/p95 e IC 95 % cuando aplique. Umbrales alineados con materialidad, riesgo y monitoreo del control interno (COSO, 2013; ISO, 2018, 2019).

4. Reproducibilidad (programa de trabajo).

La Tabla 44 vincula procedimientos con controles y evidencias asociadas, desde la perspectiva de un programa de auditoría sobre registros distribuidos.

Tabla 44
Matriz procedimiento-control (enfoque auditoría)

Procedimiento	Objetivo	Paso reproducible	Doc. soporte
---------------	----------	-------------------	--------------

Re-hash	Integridad de archivos	Calcular SHA-256 y comparar	script_rehash.py; WP-01
Inclusión (Merkle)	Pertenencia al anclaje	Validar proof vs raíz	proof_merkle.py; WP-02
Event logs	Secuencia y tiempos	Parsear y reconstruir flujo	parse_logs.py; WP-03
Conciliación	Detectar divergencias	Cruzar ERP vs anclajes	conciliacion.ipynb; WP-04

Nota. Elaboración propia, basada en principios de evidencia y programa de auditoría, y en fundamentos técnicos de hashing/árboles de Merkle y event logs (INTOSAI, 2013; ISO, 2018; Nakamoto, 2008; Wood, 2014).

B) Validación teórico–normativa

En este plano se contrasta la propuesta con:

ISSAI 100 (INTOSAI, 2013): exigencia de evidencia suficiente (cantidad) y apropiada (calidad, relevancia y fiabilidad), y de documentación que permita a otro auditor competente comprender trabajo, juicios y conclusiones.

COSO (2013): componentes de control (ambiente, evaluación de riesgos, actividades de control, información/comunicación, monitoreo) traducidos aquí en políticas de claves, segregación de funciones, observabilidad y auditorías periódicas.

Lineamientos internacionales sobre blockchain en sector público (Foro Económico Mundial & BID, 2020): gobernanza de consorcio, publicación responsable de metadatos y uso prudente de anclaje público.

La validación combina, por tanto, pruebas técnicas (contratos, hashes, inclusión, eventos, conciliaciones) con un contraste normativo explícito. El resultado esperado es que la solución propuesta no solo sea técnicamente consistente, sino que produzca evidencia apta para auditoría y rendición de cuentas, alineada con estándares reconocidos y con los objetivos de integridad y transparencia de la OA.

El capítulo metodológico define, así, un estudio de caso aplicado con enfoque mixto, delimitado institucional y técnicamente, que combina revisión documental, análisis institucional y diseño de un piloto medible. Se explicitan alcances y limitaciones, se fijan salvaguardas para validez y fiabilidad, y se detalla un programa de validación técnico–funcional y teórico–normativa que permite evaluar si la solución produce evidencia suficiente y apropiada para fines de auditoría y rendición de cuentas.

Sobre esta metodología se apoya el Capítulo 5, que desarrolla el diseño técnico de la intervención: la arquitectura híbrida on/off-chain, los módulos funcionales, los contratos inteligentes, los flujos de evidencia y las métricas operativas. Allí se concreta, en términos de componentes y controles, el marco conceptual, ético y metodológico construido en los capítulos anteriores.

4.4 Declaración de uso de inteligencia artificial

En el presente trabajo se utilizó inteligencia artificial generativa (ChatGPT, OpenAI, 2026) como herramienta de apoyo en dos instancias específicas, ambas de carácter instrumental y bajo verificación del autor.

En primer lugar, como asistencia en la elaboración de recursos visuales. Las figuras incluidas en el documento fueron generadas a partir de descripciones conceptuales (prompts) elaboradas por el autor, con el objetivo de representar arquitecturas tecnológicas, flujos de información y esquemas explicativos vinculados con los contenidos analizados. Las imágenes fueron posteriormente revisadas, ajustadas y validadas por el autor, quien definió los contenidos conceptuales representados y verificó su coherencia con las fuentes bibliográficas y el desarrollo analítico del trabajo.

En segundo lugar, como apoyo en la etapa de investigación y relevamiento. La herramienta se utilizó para la búsqueda y exploración de fuentes, antecedentes académicos, normativa y experiencias internacionales, así como para el cruce y contraste de información proveniente de distintas perspectivas. En todos los casos, las referencias identificadas a través de esta vía fueron verificadas por el autor en sus fuentes originales antes de ser incorporadas al trabajo.

La herramienta no fue utilizada para la redacción del texto ni para la elaboración de las ideas conceptuales centrales del trabajo, que son producto del trabajo intelectual del autor.

Capítulo 5: Desarrollo de la solución

5.1 Justificación del modelo híbrido

La solución propuesta adopta una arquitectura híbrida on/off chain para conciliar cuatro exigencias de la gestión pública contemporánea: (a) integridad y trazabilidad probatoria de los registros; (b) protección de datos personales y confidencialidad; (c) eficiencia operativa y cierre contable oportuno; y (d) gobernanza interinstitucional con control externo y participación ciudadana.

En términos funcionales, la capa on chain almacena huellas criptográficas (hashes), sellos de tiempo y eventos de control (alta, baja, modificación, autorización), mientras que la capa off chain resguarda datos identificatorios y documentos fuente —con firma digital válida y reglas de acceso diferenciado— en repositorios institucionales. Esta separación reduce riesgo de exposición, facilita rectificación o supresión

en la fuente cuando corresponda y preserva una cadena de custodia verificable de extremo a extremo (EDPB, 2025). La Tabla 45 resume la asignación on/off chain, su base legal y las responsabilidades asociadas.

Tabla 45

Matriz on/off chain y base legal

Artefacto	Hash	TS	Repo (OC/OF)	Base legal	DP?	Resp.	Ret.	Evid.
Expediente electrónico (PDF firmado)	SHA-256	TSP+bloque	OF: ECM/SGD; OC: anclaje	L 25.506; L 27.275; D 1023/2001	Sí	Mesa de Entradas/Compras	Cuadro institucional	Firma X.509; Merkle/txid
Acta de adjudicación/resolución	SHA-256	TSP+bloque	OF: GEDO/SGD; OC: anclaje	L 25.506; L 27.275; D 1023/2001	Sí	Autoridad competente	Normativa contractual	Firma válida; integridad OC/OF
Manifiesto de lote (raíz Merkle)	SHA-256 (raíz)	Bloque OC	OC: red pública; OF: JSON firmado	L 25.506; L 27.275	No	Operaciones/DevOps	Permanente	Verificación raíz vs. hojas; txid
Evento “Adjudicación Emitida”	Keccak-256	Bloque OC	OC: contrato; OF: indexador	L 27.275; L 25.326	No*	Equipo blockchain	Ciclo de vida	Decodificación de evento; autorización

Nota. GDE = Gestión Documental Electrónica; TAD = Trámites a Distancia; hash/digest = huella criptográfica; EIPD = Evaluación de Impacto en la Protección de Datos. Criterios: la prueba de integridad y temporalidad reside on chain; los documentos con datos personales permanecen off chain con firma digital válida. Elaboración propia con base en EDPB (2025), AAIP y URCDP (2020), Ley 25.506 (2001) y Ley 25.326 (2000).

En el plano jurídico, la validez de los documentos y asientos off chain se sostiene mediante la firma digital, cuya eficacia probatoria se equipara a la firma manuscrita. La evidencia documental se verifica

contra su digest registrado on chain, de modo que la cadena actúa como registro inmutable de integridad y temporalidad, mientras que la capa institucional conserva contenido, autoría y contexto (Ley 25.506, 2001).

La protección de datos personales se organiza bajo *privacy by design*: se evita almacenar datos identificatorios en la cadena y se prioriza el uso de evidencias (hashes, compromisos criptográficos, punteros) que remiten a la fuente original. Las autoridades de protección de datos de Argentina y Uruguay recomiendan enfoques preventivos, como la EIPD, para identificar riesgos y definir salvaguardas desde el diseño (AAIP & URCDP, 2020). El modelo híbrido incorpora desde el inicio medidas técnicas y organizativas proporcionales al riesgo —roles y políticas de acceso, cifrado en tránsito y en reposo, segregación de ambientes, registros de auditoría— y preserva la posibilidad de ejercer derechos sobre los datos en la fuente (EDPB, 2025).

En la dimensión organizacional, una red permissionada de consorcio distribuye nodos entre organismos con competencias concurrentes (tesorería, compras, auditoría interna, tribunal de cuentas, OA, entre otros), con reglas explícitas de validación, segregación de funciones y administración de identidades. Las necesidades contables (cierres periódicos, conciliaciones) exigen latencias bajas y coordinación entre múltiples actores; las arquitecturas permissionadas resultan adecuadas, mientras que el anclaje periódico de resúmenes en una red pública refuerza verificabilidad abierta y resistencia a colusiones sin sacrificar confidencialidad (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Tabla 46 detalla el esquema de anclaje híbrido.

Tabla 46
Plan de anclaje híbrido (permissionada ↔ pública)

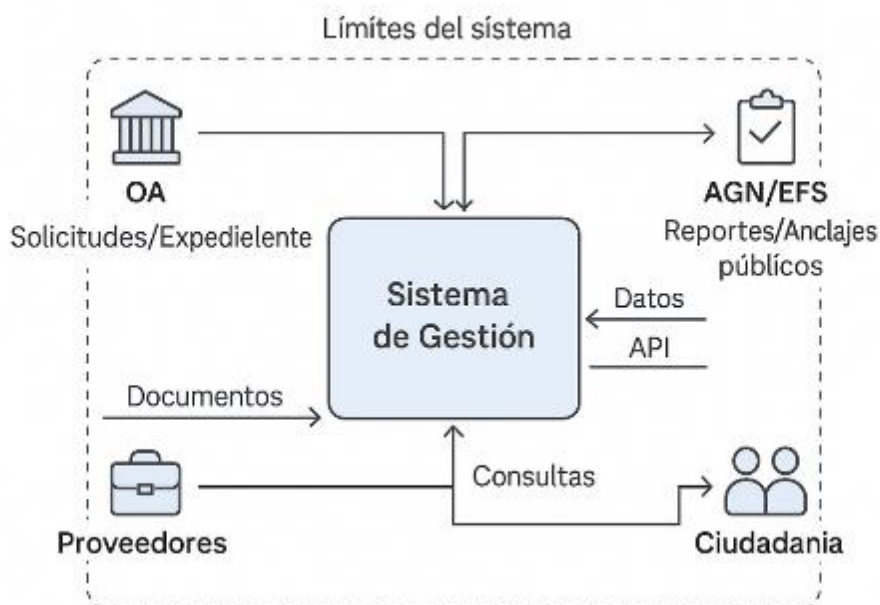
Frecuencia	Red pub. destino	Tamaño resumen	Procedimiento	Evid.	Riesgo	Mitigación
Diario	Ethereum mainnet	32 B (raíz)	Lote → firmar → enviar tx	txid; altura; manifiesto	Congestión	Multired; reintentos
Semanal	Bitcoin	32 B (raíz)	Consolidar → OP_RETURN	txid; conf.; raíz	Tarifas altas	Programación por fee
Mensual	Cadena alt.	32 B (digest)	Snapshot → anclaje	txid; snapshot	Reorg	Espera de conf.

Nota. BFT = Byzantine Fault Tolerant; PoE = prueba de existencia. Criterios: frecuencia de anclaje, red pública destino, procedimiento y mitigaciones ante fallas/colusión. Elaboración propia con base en Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Como criterio de política pública, se prioriza un despliegue incremental: piloto en procesos de alto riesgo de manipulación (por ejemplo, contrataciones y compromisos presupuestarios), medición de desempeño y calidad de datos y ampliación posterior por etapas. La evidencia comparada muestra que los beneficios aumentan cuando la solución incorpora reglas de gobernanza claras, métricas, canales de verificación ciudadana y formatos estandarizados (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). La Figura 57 muestra el diagrama de contexto del sistema propuesto, delimitando alcance, actores y principales flujos de información.

Figura 57

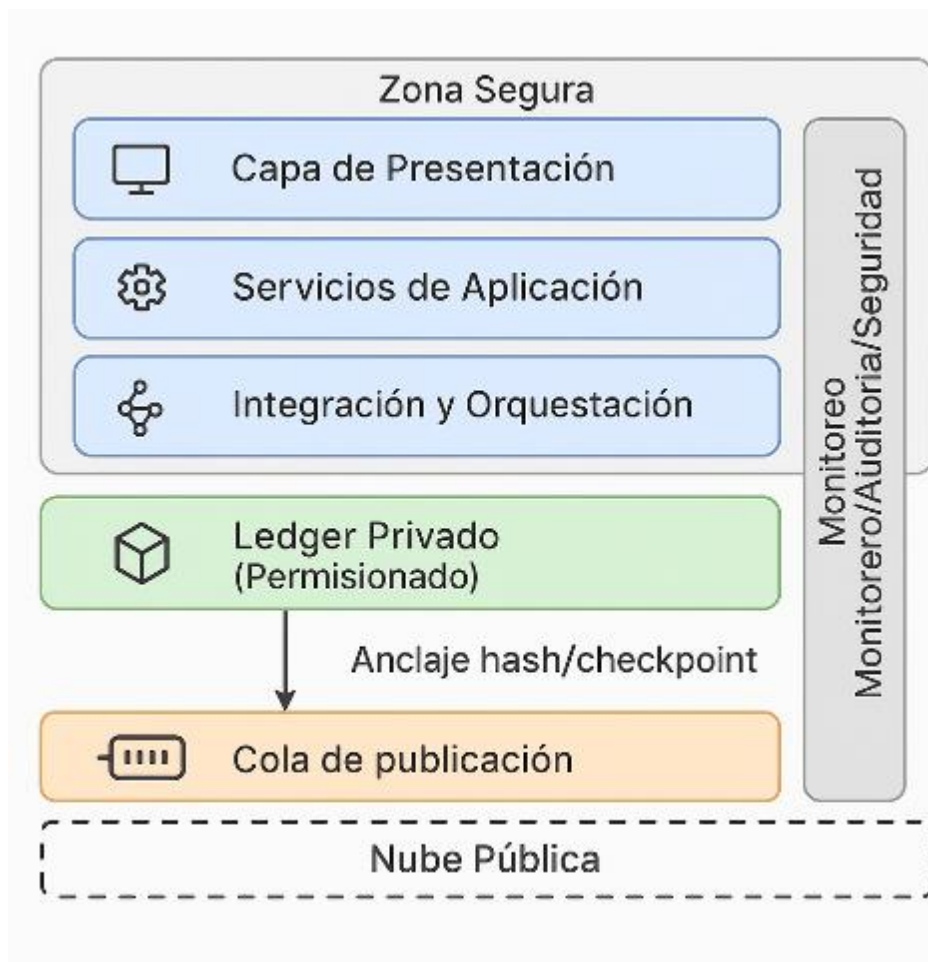
Diagrama de contexto (alcance y actores)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor.

5.2 Diseño general del sistema

La arquitectura se organiza por capas para desacoplar funciones, reducir riesgos y facilitar la auditoría continua. Cada capa aporta controles específicos y evidencias verificables que, en conjunto, satisfacen requisitos de integridad, protección de datos, eficiencia y transparencia activa. En línea con el enfoque de integridad pública de la OCDE, se adopta una perspectiva basada en riesgos y sistemas de gestión, apoyada en normas de seguridad de la información y privacidad (ISO/IEC 27001, 2022; ISO/IEC 27701, 2019; OCDE, 2020). La Figura 58 describe la arquitectura lógica de la red híbrida.

Figura 58*Arquitectura lógica de red híbrida*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con enfoque ISMS/PIMS (ISO/IEC 27001, 2022; ISO/IEC 27701, 2019) y anclaje híbrido.

(a) Capa de fuentes. Integra los sistemas operacionales (ERP financiero-contable, GDE/TAD y plataforma de contrataciones, p. ej., COMPR.AR). Cada sistema conserva documentos y datos primarios con firma digital válida y emite eventos hacia la cadena de evidencias. Se prioriza calidad de datos mediante catálogos y códigos maestros (ISO/IEC 25012, 2008).

(b) Capa de ingesta y normalización. Valida estructura y semántica de los registros, aplica reglas de negocio, mapea contra diccionarios de datos y estandariza metadatos (expediente, proveedor, partida presupuestaria). La traza de ingesta se firma y sella en tiempo para facilitar reproducibilidad y control interno (ISO/IEC 27002, 2022).

(c) Motor de evidencia. Calcula el hash del documento y de metadatos críticos, genera un sello temporal y organiza las huellas en árboles de Merkle; publica el resumen en la red permitida. El objetivo es probar existencia e integridad sin exponer datos personales o sensibles. Además, registra eventos de control (alta, baja, modificación, autorización) firmados por el sistema origen, siguiendo principios de minimización de datos y gestión de incidentes (ISO/IEC 27701, 2019; ISO/IEC 27035-1, 2023). La Tabla 47 identifica metadatos críticos y justifica su selección.

Tabla 47

Metadatos críticos y justificación de minimización

Campo	Tipo	Oblig.	Dic.	Finalidad	Base legal	Justif.	Ret.
idExpediente	string (36)	Sí	UUID	Trazabilidad	L 27.275	Vincular evidencias	Cuadro inst.
idProceso	string (24)	Sí	Código compra	Seguimiento	D 1023/2001	Trazar contratación	Normativa
hashDocumento	string (64)	Sí	SHA-256 hex	Verificación	L 25.506	Integridad sin contenido	Permanente
tsAnclaje	datetime	Sí	ISO 8601 UTC	No repudio	L 25.506	Sello verificable	Permanente
sujetoSeudon	string	No	ID seud.	Auditoría	L 25.326	Evitar PII directa	Según PIMS

Nota. ID = identificador; PII = información personal identificable. Criterios: solo se incluyen metadatos estrictamente necesarios para finalidad pública; se explicita base legal y plazo de retención. Elaboración propia con base en Ley 25.326 (2000), ISO/IEC 27701 (2019) y EDPB (2025).

(d) Contratos inteligentes. Implementan reglas de autorización, umbrales (por ejemplo, doble firma para hitos críticos), estados de ciclo (borrador, autorizado, ejecutado, observado) y controles de segregación de funciones. Registran pruebas criptográficas y metadatos no identificatorios; los datos personales permanecen en el sistema fuente bajo el PIMS (ISO/IEC 27701, 2019; ISO/IEC 27035-1, 2023).

(e) Módulo de verificación. Permite recalcular hashes, verificar inclusión en el árbol de Merkle y conciliar on/off chain (coincidencia entre digest registrado y documento firmado en el repositorio). Es utilizable por auditores internos/externos y, para datasets no sensibles, por la ciudadanía, reforzando el control social y el derecho de acceso a la información (Ley 27.275, 2016).

(f) Observabilidad y auditoría. Expone bitácoras firmadas, métricas de oportunidad y calidad, y tableros de control para SIGEN, AGN, tribunales de cuentas y OA. Los registros de auditoría se conservan con ventanas de retención acordes al marco regulatorio y controles de acceso basados en roles (ISO/IEC 27002, 2022). La Tabla 48 presenta la matriz RACI de gobernanza multi-actor.

Tabla 48

Matriz RACI de gobernanza multi-actor

Actividad	R	A	C	I	Evid./registro
Definir diccionario de metadatos	Datos	Comité	Legal	Unidades	Acta; hash versión
Gestionar claves y roles	Seguridad	CTO	Auditoría	Proveedores	Políticas; logs
Ejecutar anclaje periódico	DevOps	CTO	Seguridad	Comité	Manifiestos; txid
Revisar EIPD y salvaguardas	DPO	Comité	Seg./Legal	Unidades	Informe EIPD

Nota. RACI = RACI = Responsible, Accountable, Consulted, Informed. Criterios: segregación de funciones y registro de decisiones; se vincula cada rol con la evidencia correspondiente. Elaboración propia con base en OCDE (2020), ISO 19011 (2018) e INTOSAI (2013).

(g) Portal de consulta y apertura de datos. Publica reportes, APIs y datasets abiertos no sensibles para cumplir con transparencia activa. La información se publica en formatos abiertos, estructurados y reutilizables; el portal consume solo resultados verificados y no expone documentos con datos personales (Ley 27.275, 2016; Decreto 117/2016, 2016). La Tabla 49 alinea controles por capa con normas de seguridad, privacidad y legislación local.

Tabla 49*Controles por capa vs. ISO/IEC 27001–27701 y legislación aplicable*

Capa	Control técnico/organizativo	Norma/Art.	Evid. OC/OF	Pto. auditoría
Presentación (portal)	Accesos y sesiones; anonimización por defecto	ISO 27001 A.5.18, A.5.10; L 25.326	OF: accesos; OC: hash de releases	Altas/bajas; pruebas de sesión
Aplicación/API	Registro/monitoreo de eventos	ISO 27001 A.8.15–A.8.16	OF: SIEM/logs; OC: eventos agregados	Muestra de logs; correlación
Contratos inteligentes	Separación de funciones; control de cambios	ISO 27001 A.8.31–A.8.32; D 1023/2001	OC: tx histórico; OF: ADRs	Segregación; firma de despliegue
Datos off-chain	Clasificación; minimización; retención	ISO 27001 A.5.12; ISO 27701	OF: políticas; OC: hash de políticas	Clasificación y plazos
Infraestructura	Continuidad; copias; resiliencia	ISO 27001 A.5.30; A.8.13–A.8.14	OF: backups; OC: checksums anclados	DR y restauración
Gobierno/Personas	Transparencia activa y AIP	L 27.275; D 780/2024	OF: portal; OC: hashes datasets	Tiempos y completitud

Nota. ISMS = Information Security Management System; PIMS = Privacy Information Management System. Criterios: trazabilidad control ↔ evidencia ↔ norma; se documenta el punto de auditoría asociado. Elaboración propia con base en ISO/IEC 27001 (2022), ISO/IEC 27002 (2022), ISO/IEC 27701 (2019), Ley 27.275 (2016), Decreto 117/2016 (2016) y OCDE (2020).

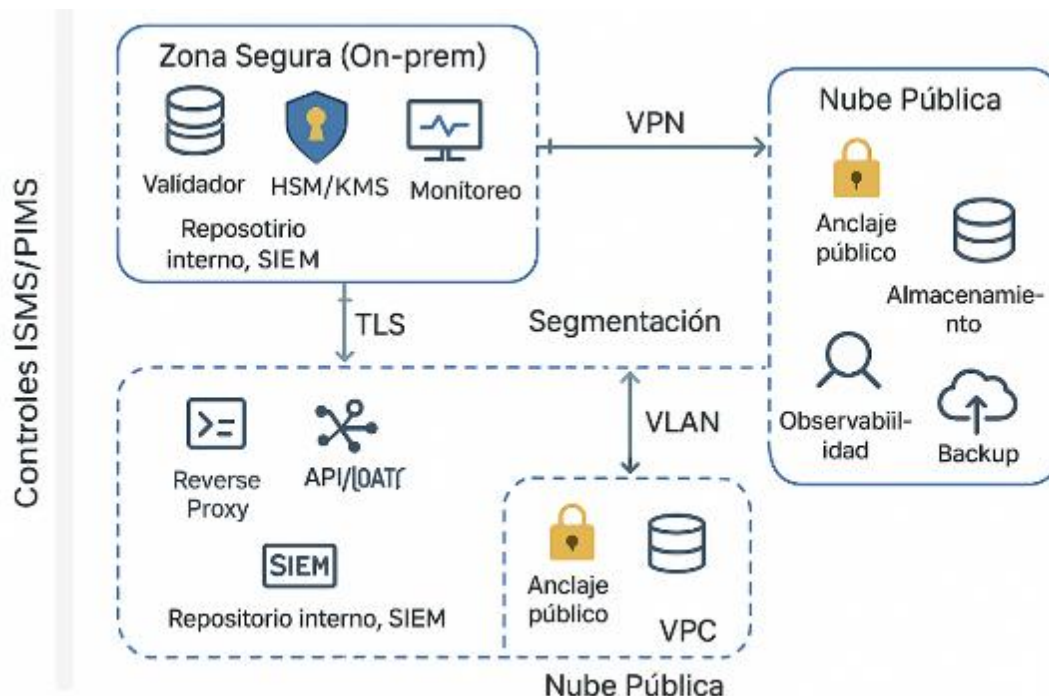
El diseño por capas habilita una cadena de custodia digital auditable que protege datos personales, mejora la eficiencia operativa y refuerza la transparencia proactiva. La arquitectura traduce obligaciones legales en controles técnicos verificables (eventos, hashes, métricas), alineando seguridad, privacidad y responsabilidad proactiva (Ley 27.275, 2016; Decreto 117/2016, 2016; ISO/IEC 27001, 2022; ISO/IEC 27002, 2022; ISO/IEC 27701, 2019; OCDE, 2020).

Tabla 50
SLO/SLA y umbrales de desempeño

Indicador	Definición	Fórmula	Objetivo	Ventana	Fuente	Resp.
Latencia de anclaje	Cierre de lote → tx minada	$t(\text{minado}) - t(\text{cierre})$	$p95 \leq 10 \text{ min}$	Diario	txid/bloque + manifiesto	DevOps
Inclusión verificable	% docs con prueba Merkle válida	$(\text{válidos/total}) \times 100$	$\geq 99,5 \%$	Semanal	Verificador reproducible	CISO
Disponibilidad portal	Uptime del portal	$(\text{min disp/total}) \times 100$	$\geq 99,8 \%$	Mensual	Monitoreo	Operaciones
Errores PII en OC	Incidentes por millón de eventos	$(\text{incidentes/eventos}) \times 10^6$	0 ppm	Mensual	Incidentes + EIPD	DPO

Nota. SLO = objetivo de nivel de servicio; SLA = acuerdo de nivel de servicio; RTO/RPO = objetivos de recuperación; p50/p95/p99 = percentiles de latencia. Criterios: métricas orientadas a cierres contables oportunos y verificación reproducible. Elaboración propia con base en ISO/IEC 27002 (2022) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

El diseño por capas habilita una cadena de custodia digital auditable que protege datos personales, mejora la eficiencia operativa y refuerza la transparencia proactiva. En términos prácticos, la arquitectura traduce obligaciones legales en controles técnicos verificables (eventos, hashes, métricas), alineando seguridad, privacidad y responsabilidad proactiva (Ley 27.275, 2016; Decreto 117/2016, 2016; ISO/IEC 27001, 2022; ISO/IEC 27002, 2022; ISO/IEC 27701, 2019; OCDE, 2020). La Figura 59 ilustra el despliegue de nodos y zonas de seguridad, incluyendo el uso de HSM/KMS para proteger claves y operaciones críticas.

Figura 59*Despliegue y seguridad (nodos, zonas, HSM/KMS)*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor alineada con ISO/IEC 27001 (2022), ISO/IEC 27701 (2019) y el mapa de controles por capa.

5.3 Módulos funcionales

Esta sección describe los módulos que materializan el diseño por capas y su correspondencia con controles de seguridad y privacidad. La lógica de ejecución es determinista y auditable: cada operación genera huellas verificables y estados observables. En términos de plataformas de contratos, Wood (2014) señala que los programas se ejecutan sobre un estado compartido y que, a partir de transacciones válidas, es posible reconstruir la historia del sistema. Esa propiedad se utiliza aquí como base para pruebas de integridad y trazas aptas para control interno y social.

Ingesta y control de calidad. Valida estructura y semántica de los registros mediante reglas de negocio, catálogos maestros (proveedores, partidas, unidades ejecutoras) y controles de duplicidad. La bitácora de ingesta se firma y sella en tiempo para asegurar reproducibilidad y auditoría. Se preservan integridad de entrada, trazabilidad de cambios y registro de excepciones (ISO/IEC 27002, 2022).

Generación de evidencias. Calcula hashes de documentos y metadatos críticos, construye árboles de Merkle y registra pruebas de inclusión con sello temporal. Emite eventos auditables (altas, bajas, modificaciones, autorizaciones) firmados por el sistema fuente. La estrategia limita el tratamiento de datos

personales en la cadena y mantiene la capacidad de verificación independiente, en línea con los principios de confidencialidad e integridad establecidos por la autoridad de protección de datos (AAIP, 2018).

Contratos inteligentes. Implementan estados y transiciones (borrador → autorizado → ejecutado → observado), listas blancas de actores, umbrales de aprobación (por ejemplo, doble firma), pausas de emergencia y gobierno de actualizaciones con separación de funciones (aprobación, revisión, despliegue). No almacenan datos personales, sino pruebas criptográficas y metadatos no identificatorios (ISO/IEC 27002, 2022; AAIP, 2018).

Verificación ciudadana y de control. Ofrece tableros con indicadores, una API para consultas automatizadas y la descarga de paquetes de verificación (documento firmado, huella y manifiesto de inclusión) para reproducir la prueba. La verificación consiste en recalcular el hash, comprobar inclusión en el árbol de Merkle y conciliar on/off chain. Se expone solo información no sensible, acorde con transparencia activa y minimización de datos (AAIP, 2018; Ley 27.275, 2016).

Monitoreo y alertas. Supervisa SLO de latencia (entre firma y registro on chain), cobertura de conciliaciones y tasa de excepciones. Emite alertas por demoras, divergencias y fallas de validación. Mantiene registros de actividad y soporta análisis forense mediante bitácoras firmadas, de acuerdo con las prácticas de la familia ISO/IEC 27000 (ISO/IEC 27002, 2022).

Gestión de claves y firmas. Administra ciclos de vida de certificados y claves con HSM/KMS, rotación programada, doble control (four eyes principle), recuperación segura y segregación de funciones (custodia, uso, auditoría). Las operaciones criptográficas se registran y se aplican políticas de cifrado, control de acceso y registro de eventos, consistentes con los lineamientos de la AAIP y los controles de criptografía y gestión de claves de ISO/IEC 27002 (AAIP, 2018; ISO/IEC 27002, 2022).

La Tabla 51 resume los eventos de los contratos inteligentes y el esquema de registro asociado, clave para la auditoría técnica.

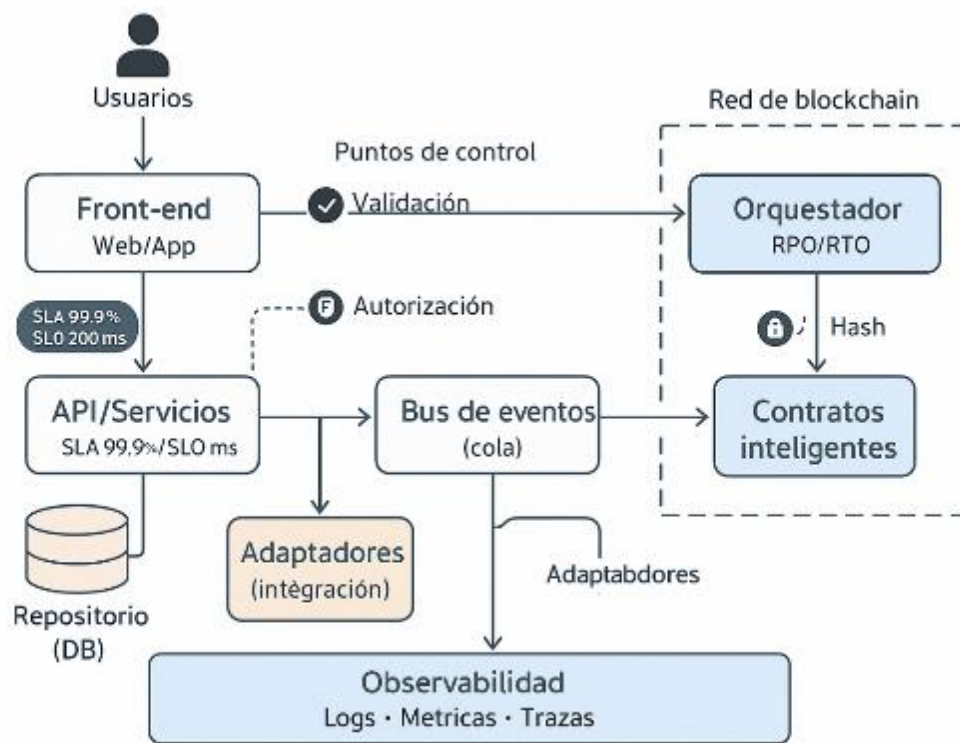
Tabla 51*Eventos de contrato inteligente y esquema de registro (log)*

Evento	Desc.	Campos	Tipo	Estado prev/post	Cto. origen	Regla auth.
Adjudicacion Emitida	Emisión acto	idProceso, idExpediente , hashActo	bytes32, bytes32, bytes32	Evaluable → Adjudicado	ProcContrata ciones	MULTISIG(2/3)
RecepcionOf erta	Registro de oferta	idProceso, hashOferta	bytes32, bytes32	Apertura → Recibida	ProcContrata ciones	Rol Oferente + validador
AnclajeLote	Publicación raíz Merkle	raizMerkle, periodo	bytes32, uint256	Pendiente → Anclado	Anclaje	Rol Operaciones
RevocacionA cceso	Revocación permisos	idUsuario, rol	address, string	Habilitado → Revocado	GobiernoAcc esos	MULTISIG(2/3)

Nota. VM = máquina virtual; ABI = interfaz binaria de aplicación. Criterios: cada transición emite evento con sello temporal, IDs y digest; los eventos no almacenan datos personales. Elaboración propia con base en Wood (2014), ISO/IEC 27002 (2022) y AAIP (2018).

La Figura 60 presenta, en visión C4-Container, los componentes y módulos del sistema y sus principales interacciones.

Figura 60
Componentes y módulos (visión C4-Container)

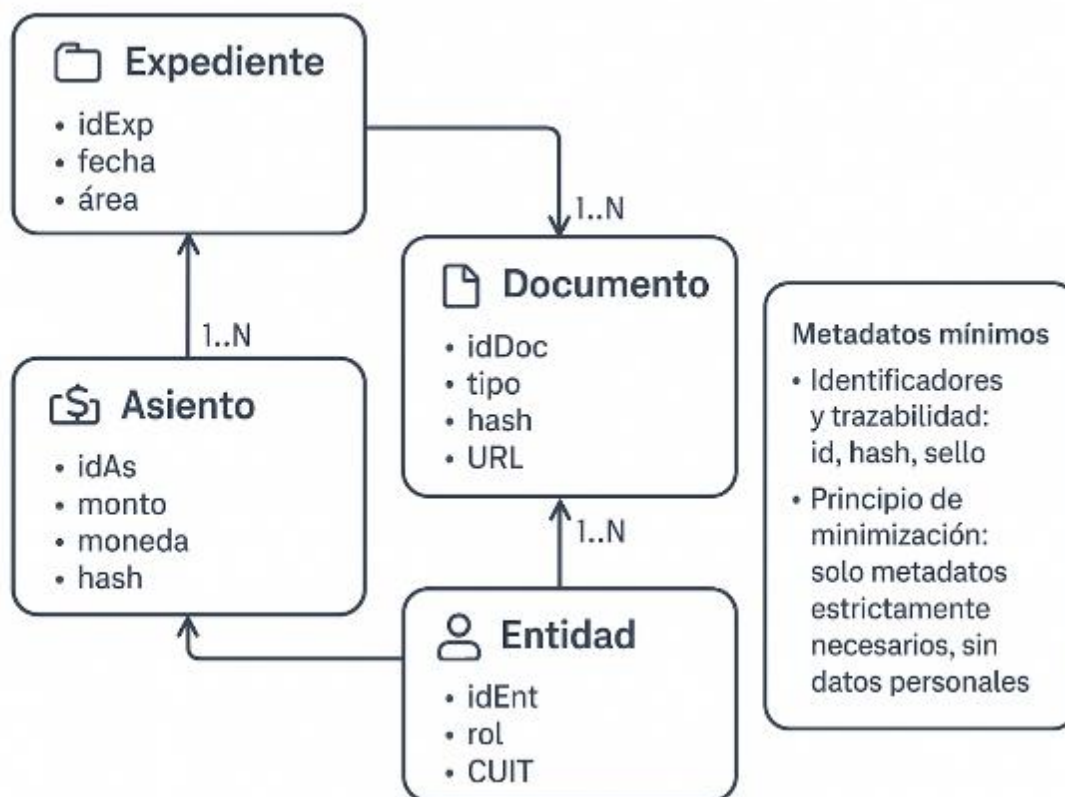


Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor.

En conjunto, los módulos proveen evidencia técnica que vincula la lógica de negocio con una cadena de custodia verificable. Los contratos ejecutan código de forma determinista sobre un estado compartido y dejan un rastro que soporta auditoría y participación social (Wood, 2014). La arquitectura convierte obligaciones legales y de gestión en controles operativos medibles, alineando seguridad, privacidad y transparencia.

5.4 Protección de la información

La protección de la información se rige por el principio CIA (confidencialidad, integridad, disponibilidad), el mínimo privilegio, la segregación de funciones y la defensa en profundidad. El tratamiento adopta un enfoque basado en riesgos que articula controles organizativos y técnicos proporcionales a la sensibilidad y al impacto. En materia de datos personales, AAIP & URCDP (2020) subrayan la importancia de evaluar anticipadamente los riesgos y documentar salvaguardas mediante instrumentos como la EIPD (ver Figura 61).

Figura 61*Modelo de datos y metadatos mínimos (ER)*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor conforme a principios de privacidad por diseño (ISO/IEC 27701, 2019; Ley 25.326, 2000) y controles por capa.

Minimización y partición on/off chain. Los datos personales permanecen fuera de la cadena; en la cadena solo se registran evidencias criptográficas y metadatos estrictamente necesarios para probar integridad, existencia y temporalidad. La Ley 25.326 exige que los datos sean adecuados, pertinentes y no excesivos en relación con la finalidad del tratamiento (Ley 25.326, 2000). La partición on/off chain se diseña precisamente para cumplir este criterio y, al mismo tiempo, preservar la auditabilidad.

Controles organizativos y técnicos. Para operaciones de alto riesgo se requiere una EIPD documentada con identificación de riesgos residuales y medidas compensatorias (AAIP & URCDP, 2020). Entre las medidas técnicas se incluyen cifrado en tránsito y en reposo, control de accesos basado en roles, registro de actividad y trazabilidad de eventos, políticas de retención y destrucción segura, y revisiones periódicas de eficacia. El estándar ISO/IEC 27701 complementa estos controles definiendo roles, procedimientos y salvaguardas para información personal identificable y alineando el principio de

minimización con mecanismos de seguridad y privacy by design (ISO/IEC 27701, 2019). La Tabla 52 resume los principales riesgos identificados por módulo, las salvaguardas previstas y el riesgo residual.

Tabla 52

Riesgos y salvaguardas EIPD por módulo

Riesgo	Prob.	Imp.	Salvaguarda	Resp.	Evid.	Estado
Reidentificación por correlación de metadatos OC	M	A	Seudonimización; sal/HMAC; lotes Merkle	DPO/Tratamiento	Informe EIPD; pruebas	En curso
Publicación accidental de datos personales en OC	A	A	Validaciones en contratos; metadatos-only; 4 ojos; gates CI/CD	PO/DPO	Checklist; auditoría código	Abierto
Integridad de evidencias OF comprometida	M	A	WORM; firmas; anclaje periódico; logging	CISO	Registros firmados; verificación	Mitigado
Indisponibilidad/congestión de red pública	B	M	Multianclaje; colas; reintentos; diferido	DevOps	Runbooks; SLO	En curso

Nota. EIPD = Evaluación de Impacto en la Protección de Datos; ISMS = Sistema de Gestión de Seguridad de la Información; PIMS = Sistema de Gestión de Información de Privacidad. Escalas: probabilidad e impacto en niveles 1–5; riesgo residual tras salvaguardas. Elaboración propia con base en AAIP y URCDP (2020), ISO/IEC 27701 (2019) e ISO/IEC 27002 (2022).

Gestión de claves, firmas y evidencias. La custodia de claves se realiza con HSM/KMS, rotación programada, doble control y segregación de funciones. Las operaciones criptográficas se registran en bitácoras firmadas y selladas, preservando una cadena de custodia verificable. Este esquema reduce la superficie de ataque y facilita la auditoría de controles criptográficos (ISO/IEC 27701, 2019; ISO/IEC 27002, 2022).

La combinación de minimización, partición on/off chain y controles PIMS/ISMS convierte obligaciones legales en mecanismos observables: la ciudadanía puede reproducir pruebas de integridad sin

exponer datos personales; los organismos de control acceden a trazas completas; y los titulares conservan su capacidad de ejercer derechos sobre la fuente, con seguridad y responsabilidad proactiva (AAIP & URCDP, 2020; EDPB, 2025; ISO/IEC 27701, 2019).

5.5 Contratos inteligentes y validación

Los contratos inteligentes materializan reglas de negocio en código ejecutado de forma determinista sobre un estado compartido, dejando un rastro verificable que vincula lógica y evidencia técnica. Para asegurar su confiabilidad, el ciclo de vida combina prácticas de desarrollo seguro, controles organizativos y auditorías independientes. Las normas de auditoría de sistemas de gestión enfatizan la necesidad de obtener evidencia suficiente y apropiada para sustentar conclusiones, criterio también adoptado en el sector público (ISO 19011, 2018; INTOSAI, 2013). La Figura 62 grafica la secuencia del registro contable de principio a fin junto con los actores involucrados.

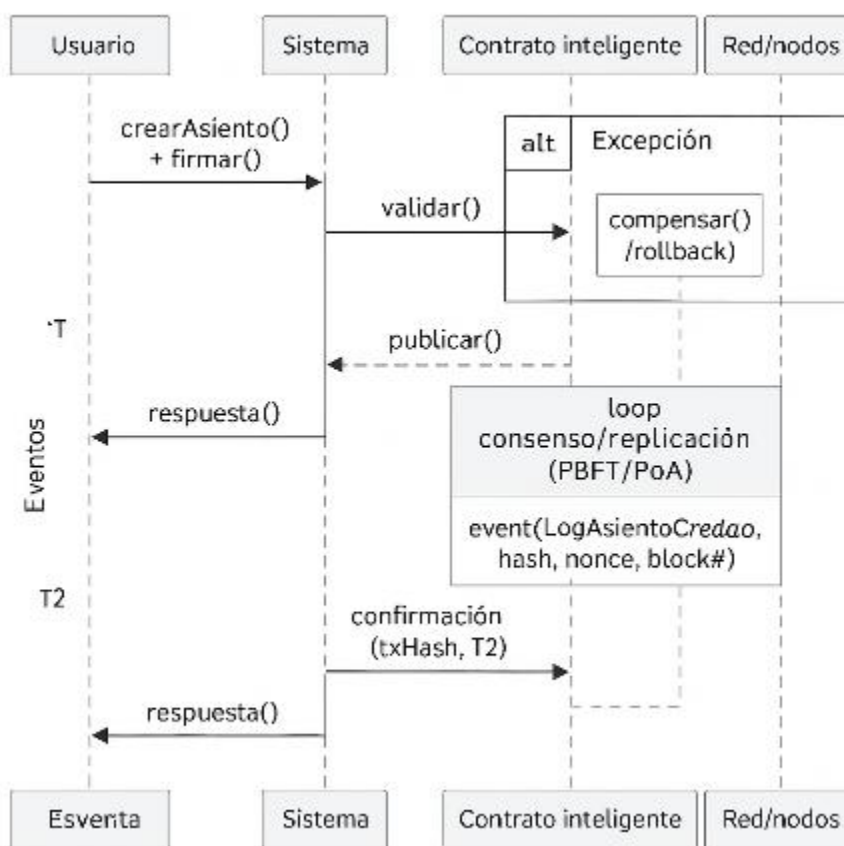
El ciclo de vida de los contratos incluye las prácticas de desarrollo seguro: (a) pruebas unitarias e integración con criterios de cobertura; (b) linters y análisis estático para detectar vulnerabilidades; (c) cobertura de casos adversos (reentradas, errores de autorización, desbordamientos, límites de gas); (d) eventos normalizados para cada hito relevante; (e) mecanismo de actualización con bloqueos temporales (timelocks) y aprobación multirol; y (f) verificación independiente mediante guías reproducibles.

Estas prácticas reducen riesgo de defectos latentes y facilitan auditorías reiterables (ISO 19011, 2018; INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Trazabilidad y eventos. Cada transición de estado emite un evento con identificadores, sello temporal del bloque y digest asociado. Los eventos se diseñan con esquemas estables (nombre, campos, tipos, códigos de resultado) para permitir lectura automatizada y vinculación con artefactos off chain (manifiestos, bitácoras de ingesta). Esto habilita pruebas sobre poblaciones completas, reforzando la solidez de la evidencia (INTOSAI, 2013).

Figura 62

Secuencia del registro contable con smart contracts (UML)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en especificaciones de máquina virtual y registros de eventos (Wood, 2014; ISO/IEC 27002, 2022; AAIP, 2018).

Gobierno de actualizaciones. Las modificaciones de código se gobiernan mediante contratos proxy con bloqueo temporal, aprobación por múltiples roles (dueño funcional, responsable de seguridad, auditor interno) y ventanas de observación antes del cambio efectivo. La separación de funciones y la trazabilidad de decisiones se registran en eventos y documentación de auditoría (ISO 19011, 2018).

Validación técnico-funcional. La validación integra pruebas criptográficas y funcionales: recálculo de huellas de documentos/actas y comparación con el digest registrado; pruebas de inclusión en el árbol de Merkle y verificación de cabeceras; lectura de event logs y reconstrucción de estados; conciliación on/off chain entre eventos blockchain y asientos/documentos en repositorios institucionales; métricas de latencia (firma → hash on chain), cobertura de conciliaciones y tasa de excepciones.

Auditoría y verificación independiente. Se proveen guías de trabajo reproducibles para equipos internos y externos, con datasets de evidencia, scripts de verificación y criterios de aceptación. Las normas del sector público requieren que el trabajo del auditor sea planificado, se ejecute con escepticismo profesional y se documente con evidencia suficiente y apropiada, de manera que otro profesional competente pueda comprender hallazgos y fundamentos (INTOSAI, 2013; ISO 19011, 2018).

En el contexto de contrataciones públicas con blockchain, el Foro Económico Mundial y el BID (2020) indican que los registros deben ser legibles por máquinas, las verificaciones reproducibles por terceros y los estados trazables de principio a fin, minimizando al mismo tiempo la información personal en la cadena. La combinación de pruebas sistemáticas, análisis estático, eventos normalizados, gobierno de actualizaciones y auditoría independiente busca ese equilibrio. La validación técnico-funcional —re-hash, inclusión, lectura de eventos y conciliación on/off chain— se mide con métricas de latencia y cobertura y se alinea con las buenas prácticas de auditoría, garantizando que los contratos inteligentes no solo funcionen, sino que generen evidencia adecuada para la rendición de cuentas (ISO 19011, 2018; INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

5.6 Participación ciudadana e incentivos

La participación ciudadana se operacionaliza mediante publicación proactiva de información no sensible, formatos abiertos reutilizables, métricas explicables y canales de retroalimentación trazables. El objetivo es habilitar control social efectivo, estimular mejoras continuas y asegurar inclusión de personas y grupos históricamente subatendidos. La ley de acceso a la información pública establece como finalidad garantizar el ejercicio de ese derecho y la transparencia de la gestión (Ley 27.275, 2016).

Apertura de información y datasets. Se publicarán métricas no sensibles, datasets con metadatos y versionado, y reportes explicables que detallen reglas, supuestos y límites metodológicos. La información se liberará en formatos abiertos y legibles por máquinas, con diccionarios de datos, historial de cambios y sellos de tiempo. La OCDE subraya que la integridad pública requiere datos accesibles y comprensibles que permitan escrutinio y aprendizaje institucional (OCDE, 2020). La Tabla 53 clasifica los datasets previstos para transparencia activa según sensibilidad y condiciones de publicación y acceso.

Tabla 53
Datasets de transparencia activa y sensibilidad

Dataset	Periodic.	Sens.	Formato	Dic.	Ruta legal	Publ.
Contratos adjudicados	Mensual	Medio	CSV/JSON	idProceso, monto, proveedor	L 27.275	Sí
Órdenes de pago	Mensual	Alto	CSV/JSON	idOrden, fecha, monto	L 27.275; L 25.326	Sí (agregados)
Licitaciones en curso	Semanal	Bajo	JSON	idProceso, estado	L 27.275	Sí
Auditorías realizadas	Trimestral	Medio	PDF/JSON	idAuditoría, hallazgos	L 27.275	Sí

Nota. OA = Oficina Anticorrupción; API = interfaz de programación de aplicaciones. Criterios: publicación en formatos abiertos, diccionarios de datos y versionado, excluyendo PII. Elaboración propia con base en Ley 27.275 (2016) y Decreto 117/2016 (2016).

Canales de participación y retroalimentación. El portal ofrecerá formularios, API y mecanismos de comentarios para señalamientos de inconsistencias, solicitudes de mejora y alertas de interés público. Cada aporte ciudadano generará un ticket trazable con estado (recibido, en análisis, resuelto), plazos y evidencia asociada. La respuesta institucional alimentará los tableros, favoreciendo ciclos de mejora continua (Ley 27.275, 2016).

Incentivos no monetarios. Se prevén sellos de cumplimiento y reconocimientos públicos para equipos con mejores tiempos de cierre y verificación, mayor cobertura de conciliaciones y mejor calidad de datos. Estos incentivos se comunican en el portal y en informes periódicos; se busca alinear reputación y conducta prointegridad sin introducir recompensas económicas (OCDE, 2020).

Accesibilidad universal y lenguaje claro. La publicación y los canales de interacción observarán el principio de accesibilidad y de lenguaje claro, evitando barreras técnicas o lingüísticas y habilitando canales alternativos (telefónicos o presenciales) para no excluir a grupos vulnerables. La Ley 26.653 (2010) dispone que las páginas de internet de organismos públicos deben cumplir condiciones de accesibilidad para que todas las personas, incluidas aquellas con discapacidad, puedan acceder a la información en forma autónoma y sin discriminación.

Trazabilidad y métricas de participación. Se publicarán indicadores como: número de descargas de paquetes de verificación, tasa de re-hash reproducidos por terceros, cobertura de conciliaciones on/off

chain, tiempos de respuesta a reportes ciudadanos y porcentaje de incidencias resueltas. Estas métricas se presentarán en series temporales y desagregadas (organismo, proceso, etapa), de modo que el control social sea verificable y replicable por actores externos (Ley 27.275, 2016; OCDE, 2020). La Tabla 54 define métricas de participación y control social.

Tabla 54

Métricas de participación y control social

Métrica	Def. operacional	Meta	Periodic.	Fuente	Segm. (org./proc.)
Respuestas en plazo AIP	% solicitudes $\leq$ plazo legal	≥ 95 %	Mensual	Gestor AIP	Por organismo
Uso de verificadores	# descargas/ejecuciones	+20 % trimestral	Trimestral	Portal/repo	Por proceso
Participación en consultas	# aportes válidos	≥ 50 /consulta	Por consulta	Plataforma	Por tema
Calidad de datasets	% con diccionario completo	100 %	Trimestral	QA de datos	Por organismo

NotaKPI = indicador clave de desempeño. Criterios: definiciones operacionales, periodicidad y segmentación para escrutinio externo replicable. Elaboración propia con base en Ley 27.275 (2016) y OCDE (2020).

La combinación de datos abiertos versionados, reportes explicables, canales trazables e incentivos no monetarios crea mecanismos de rendición de cuentas que fortalecen la integridad pública.

5.7 Casos de uso y simulaciones

Los casos piloto priorizan procesos de alto impacto en integridad y trazabilidad: (a) comprobantes contables de alto volumen (compromisos, devengados, órdenes de pago) para validar escalabilidad y conciliación masiva; (b) hitos de compras públicas (pliegos, ofertas, aperturas, actas y adjudicaciones) para auditar secuencias y tiempos críticos; y (c) certificaciones documentales (resoluciones, informes, dictámenes) para verificar integridad y autoría a partir de evidencias criptográficas. La premisa es que la evidencia debe ser suficiente y apropiada para sustentar conclusiones y rendición de cuentas (INTOSAI, 2013; ISO 19011, 2018).

Diseño de simulaciones. Se ejecutarán pruebas de carga y estrés, demoras de red, fallos de nodo (incluido comportamiento bizantino simulado) y pruebas de finalidad en protocolos BFT permissionados. Cada escenario define población, parámetros, duración, repetición y criterios de aceptación. La evidencia resultante documenta latencia (p50/p95/p99 firma $\rightarrow$ hash on chain), throughput (transacciones/segundo), tasa de excepciones (validación, autorización, conciliación), tiempo a finalidad, recuperación ante incidentes (RTO/RPO) y cobertura de conciliaciones on/off chain.

Criterios de aceptación estimados:

Finalidad ≤ 5 s en BFT permissionado con ≥ 4 nodos validadores y ≥ 1 nodo caído.

Latencia firma $\rightarrow$ registro on chain ≤ 3 min (p95) para lotes de 10.000 comprobantes.

Cobertura de conciliaciones $\geq 99,95$ % en poblaciones completas; divergencias documentadas con causa y remediación.

Recuperación de nodo validador ≤ 10 min con resincronización completa y sin pérdida de evidencia.

La Tabla 55 detalla los parámetros de las simulaciones de desempeño y los criterios de aceptación asociados para el entorno piloto.

Tabla 55

Simulaciones: parámetros y criterios de aceptación

Prueba	Pob./seed	Parámetros	Dur.	Criterio	Esperado
Carga masiva de evidencias	42	n=10.000; tamaño=200 KB	2 h	p95 ≤ 10 min	Cumple
Reorg moderada	1337	profundidad=2 bloques	1 h	Sin pérdida de integridad	Cumple
Fuga accidental de PII	2025	tasa error=1e-6	30 min	0 eventos en OC	Cumple
Caída de red destino	314	downtime=30 min	1 h	Reintento ≤ 15 min	Cumple

Nota. TPS = transacciones por segundo; p95/p99 = percentiles; RTO/RPO = objetivos de recuperación. Criterios: escenarios de carga, fallos de nodo y finalidad observada en BFT permissionado. Elaboración propia con base en INTOSAI (2013), ISO 19011 (2018) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020).

Metodología y reproducibilidad. Las simulaciones se instrumentan con datos sintéticos representativos o datos anonimizados, seeds y manifiestos de corrida (configuración, versión de contratos, commits, horario). Se genera un paquete de evidencia por experimento: bitácoras firmadas, métricas,

capturas de eventos y resultados de verificación (re-cálculo de hash, prueba de inclusión y conciliación). Según ISO 19011 (2018), la evidencia de auditoría debe ser pertinente, verificable y suficientemente documentada para permitir su evaluación por terceros. La Tabla 56 enumera las verificaciones reproducibles previstas.

Tabla 56
Catálogo de verificaciones reproducibles

Prueba	Herramienta	Entrada	Salida esp.	Reprod.	Evid. pkg.
Verificación de inclusión Merkle	Script CLI	manifiesto.json, prueba.json	true/false + ruta	1-clic/script	.zip con hash
Verificación de firma digital	Validador X.509	PDF firmado	sello válido + cadena	1-clic/script	PDF + log + huellas
Reconciliación OC/OF	Comparador	hash OF vs. evento OC	0 desvíos	1-clic/script	CSV de coincidencias
Auditoría de roles	Auditor RBAC	snapshot de permisos	diffs autorizados	1-clic/script	reporte firmado

Nota. PoE = prueba de existencia; PoI = prueba de inclusión (árbol de Merkle). Criterios: para cada verificación se documentan entradas, salidas esperadas y evidencia empaquetada (manifiesto, bitácoras, hashes). Elaboración propia con base en ISO 19011 (2018) y Wood (2014).

Ruta de validación cruzada. Se habilitan guías reproducibles para que equipos de auditoría y control externo repliquen las pruebas: scripts de lectura de event logs, verificadores de inclusión y conciliadores. Esto permite corroboración independiente y análisis de sensibilidad (cambios en parámetros, topologías y fallos) con trazabilidad completa de decisiones (INTOSAI, 2013).

Justificación del uso de BFT permissionado. Los protocolos de tolerancia a fallos bizantinos (BFT) en redes de consorcio priorizan finalidad rápida y gobernanza multi-actor, lo que resulta adecuado para cierres contables y control concurrente. El Foro Económico Mundial y el BID (2020) destacan que estos protocolos pueden ofrecer finalidad en segundos y facilitar mecanismos de gobernanza compartida.

Los casos piloto y las simulaciones constituyen un banco de pruebas que conecta objetivos de integridad con evidencia verificable y criterios de aceptación claros. La combinación de métricas (latencia, throughput, finalidad, excepciones), reproducibilidad y validación cruzada se alinea con el estándar de

evidencia suficiente y apropiada para auditoría y rendición de cuentas (INTOSAI, 2013; ISO 19011, 2018; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

5.8 Diagramas técnicos

Para asegurar replicabilidad y revisión por terceros, se incorporan diagramas normalizados que documentan alcance, estructura y comportamiento del sistema, así como el flujo de evidencias y controles asociados. Estos artefactos se producen respetando el ancho útil de 16,51 cm, con pie de figura en el texto, numeración correlativa y referencias cruzadas desde el cuerpo principal. Los recursos gráficos ayudan a presentar de manera esquemática el procedimiento general y el tipo de diseño aplicado (Sabino, 2014) y, en ingeniería de software, se integran en puntos de vista arquitectónicos coherentes (ISO/IEC/IEEE 42010, 2011).

Los diagramas previstos son:

Diagrama de contexto. Representa actores (organismos, ciudadanía, auditores), límites del sistema e interacciones principales. Objetivo: fijar alcance y responsabilidades.

Diagrama de componentes. Estructura servicios, contratos inteligentes, repositorios y adaptadores. Objetivo: explicitar dependencias y puntos de control.

Diagramas de secuencia. Describen los pasos crear/firmar → validar/publicar → consensuar/replicar, incluyendo eventos, sellos de tiempo y errores previstos. Objetivo: verificar determinismo, idempotencia y trazabilidad.

Modelo de datos. Detalla metadatos y diccionarios (identificadores, catálogos maestros, estados, códigos). Objetivo: asegurar calidad y consistencia semántica.

Diagrama de despliegue. Ubica nodos, redes, zonas de seguridad, HSM/KMS, monitoreo y backups. Objetivo: mostrar controles de seguridad y continuidad.

Flujo de evidencia. Mapea hashes, pruebas de inclusión, eventos, verificación y conciliación on/off chain. Objetivo: vincular decisión de negocio, evidencia técnica y norma aplicable.

Alineación con marcos de ciberseguridad. Cada diagrama indicará su relación con las funciones del Marco de Ciberseguridad de NIST: identificar, proteger, detectar, responder y recuperar. El marco presenta estas funciones como categorías complementarias para gestionar riesgo y resiliencia con un lenguaje común entre áreas técnicas y de gestión (NIST, 2018).

Convenciones de notación y control de cambios. Se utilizarán convenciones homogéneas (nombres, estereotipos, colores funcionales, leyendas) y versionado semántico de los artefactos. Cada diagrama incluirá fecha, versión, autores y revisores, y quedará asociado a decisiones arquitectónicas (ADR) con su

justificación. Un diseño claro y consistente facilita que terceros comprendan la solución sin ambigüedades (Sabino, 2014).

Trazabilidad y verificabilidad. Todos los artefactos mantendrán trazabilidad bidireccional hacia requisitos, controles y evidencias: requisito → diseño → contrato/evento → verificación, y verificación → evento/contrato → diseño → requisito. Este encadenamiento permite que revisores externos reconstruyan decisiones y comprueben conformidad con criterios (ISO/IEC/IEEE 42010, 2011).

El paquete de diagramas técnicos documenta alcance, estructura, comportamiento, datos, despliegue y evidencia en un formato reproducible y auditable. Conecta decisiones de diseño con controles y resultados esperados y facilita la revisión externa al proporcionar un lenguaje gráfico común entre actores (NIST, 2018; ISO/IEC/IEEE 42010, 2011; Sabino, 2014).

Capítulo 6: Plan de implementación

Este capítulo descende de la propuesta a la práctica: define el alcance institucional, su secuencia de despliegue, los recursos y costos involucrados, los requisitos legales y de gobernanza, los instrumentos e indicadores de éxito, el plan de gestión del cambio y un registro de riesgos con sus estrategias de mitigación. La solución se validará en un proceso de alto impacto de la Oficina Anticorrupción (OA) mediante una arquitectura híbrida: red permitida para la operación diaria y anclaje periódico de huellas (hashes, sellos de tiempo y estados) en una cadena pública, conciliando integridad verificable con resguardo de la confidencialidad (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; INTOSAI, 2013).

El diseño sigue tres principios rectores: (i) publicación mínima verificable (metadatos y huellas on-chain; documentos íntegros y datos personales off-chain bajo control de acceso), (ii) gobernanza explícita (membresías, quóruns y segregación de funciones alineados con marcos COSO/ISSAI), y (iii) medición reproducible (latencia documento→anclaje, cobertura de asientos con hash verificable, discrepancias on/off-chain y trazabilidad de eventos). Estos principios se operacionalizan en controles programables y evidencias auditables, evitando el “tecnosolucionismo” y orientando el valor al desempeño observable del sistema de registro (INTOSAI, 2013).

Como hilo conductor de ciberseguridad y resiliencia operativa, se integra el Marco de Ciberseguridad del NIST a lo largo del ciclo de vida: Identificar (activos, riesgos y dependencias), Proteger (controles ex ante y resguardo de datos), Detectar (monitoreo de eventos y anomalías), Responder (procedimientos y quóruns ante incidentes) y Recuperar (continuidad y evidencia post-evento). Estas funciones operan de forma concurrente y continua, promoviendo una cultura de control medible y verificable (NIST, 2018, pp. 7–8).

En términos de comunicación técnica y trazabilidad documental, se adoptan convenciones homogéneas (nomenclatura, estereotipos, colores funcionales, leyendas y versionado semántico), de modo tal que cada artefacto de diseño (diagramas, decisiones arquitectónicas y contratos inteligentes) mantenga trazabilidad bidireccional con requisitos, controles y evidencias. Se asume, en consecuencia, que “el diseño debe exhibir una forma unitaria y lógica, de manera que pueda ser comprendido sin ambigüedades” (Sabino, 2014, p. 49), criterio que guía tanto la redacción como la presentación visual del capítulo.

Sobre esta base, el capítulo se organiza en ocho apartados: la elección del organismo y del proceso objetivo (6.1); las etapas del despliegue con entregables y criterios de salida (6.2); los recursos humanos requeridos y su RACI (6.3); la infraestructura tecnológica y costos (6.4); los aspectos legales y regulatorios habilitantes y sus salvaguardas (6.5); los indicadores y métodos de medición (6.6); el plan de gestión del cambio y capacitación (6.7); y el registro de riesgos y mitigaciones (6.8). Este itinerario conecta decisiones de diseño con resultados verificables, asegurando que sea auditado, medido y transferible a otras dependencias públicas bajo los mismos criterios de evidencia y control (BID, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; INTOSAI, 2013; NIST, 2018; Sabino, 2014).

6.1 Elección del organismo público

6.1.1 La Oficina Anticorrupción: historia y creación

La Oficina Anticorrupción (OA) es un organismo desconcentrado del Ministerio de Justicia y Derechos Humanos con mandato de prevención, investigación preliminar y formulación de políticas de integridad en el ámbito de la Administración Pública Nacional. Su creación, objeto, competencias y estructura quedaron establecidos por el Decreto 102/1999, que la institucionalizó como nodo especializado del ecosistema de integridad y control del Poder Ejecutivo Nacional (Ley 25.188, 1999). La misión, servicios y líneas de trabajo se sintetizan en su portal institucional (OA, s. f.). En su encuadre sistémico, la OA articula con el control interno (SIGEN) y el control externo (AGN), en armonía con los principios y prácticas definidos por la Ley 24.156 de administración financiera y de los sistemas de control del sector público (Ley 24.156, 1992).

6.1.2 Cómo funcionan hoy sus procesos (síntesis operativa)

Denuncias e investigaciones. La OA recibe denuncias en línea, presencial o postal, admitiendo modalidades anónima, con identidad reservada o con identificación. Luego del control de admisibilidad, puede abrir investigación preliminar, requerir información a organismos y, cuando corresponde, formular denuncia penal y/o constituirse en querellante, según su marco competencial (Ley 25.188, 1999; OA, s. f.).

Declaraciones Juradas Patrimoniales Integrales (DDJJ). La OA administra el régimen de DDJJ para altos cargos, con presentación en ARCA–AFIP (Form. F.1245 y, cuando corresponde, F.1246), publicación con resguardos legales y coordinación con áreas de personal. En 2025, la OA prorrogó el vencimiento de la obligación anual 2024 hasta el 31/07/2025 (OA, 2025; AFIP, s. f.; OA, s. f.; Ley 25.188, 1999).

Registros de obsequios y de viajes financiados por terceros. La OA gestiona los registros creados por el Decreto 1179/2016 (reglamentario del art. 18 de la Ley 25.188): valida las cargas y publica la información como instrumento de transparencia activa (Decreto 1179/2016, 2016; Ley 25.188, 1999; OA, s. f.).

Marco habilitante transversal. El funcionamiento se apoya en la Ley 25.188 (ética pública), la Ley 24.156 (administración financiera y control), la Ley 25.326 (protección de datos personales y su reglamentación) y la Ley 25.506 (firma digital y su reglamentación), que habilitan firma digital, sellado de tiempo, publicación con accesos diferenciados y resguardo de datos personales (Ley 25.188, 1999; Ley 24.156, 1992; Ley 25.326, 2000; Ley 25.506, 2001).

6.1.3 Criterios de selección de la OA

a) Mandato y transversalidad. Competencia explícita en integridad pública y prevención de la corrupción, con impacto sistémico y reputacional dentro de la APN (Ley 25.188, 1999; OA, s. f.).

b) Articulación con el sistema de control. Interoperabilidad con SIGEN (control interno) y AGN (control externo), pilares de la Ley 24.156 (Ley 24.156, 1992).

c) Procesos con evidencia trazable. Denuncias/investigaciones, DDJJ y registros de obsequios/viajes generan rastros documentales y metadatos donde inmutabilidad, sellado de tiempo y versionado elevan auditabilidad y valor probatorio (Ley 24.156, 1992; Ley 25.188, 1999; Decreto 1179/2016, 2016).

d) Factibilidad jurídica y técnica. Operación con firma digital/sellado, publicación selectiva y accesos diferenciados que resguardan datos personales (Ley 25.506, 2001; Ley 25.326, 2000).

e) Transparencia activa existente. Publicaciones y datasets (DDJJ; obsequios/viajes) que facilitan verificación pública y trazabilidad externa (OA, s. f.; Decreto 1179/2016, 2016).

f) Medición objetiva. Posibilidad de fijar indicadores verificables (p. ej., cobertura de hitos con hash, latencia documento→anclaje, divergencias on/off-chain, aceptación de auditoría), alineables con marcos de control y auditoría (INTOSAI, 2013).

g) Escalabilidad. Potencial de réplica a otros organismos con ajustes mínimos, al apoyarse en normas marco y prácticas vigentes (Ley 24.156, 1992; Ley 25.188, 1999).

6.1.4 Implementación en los procesos actuales

Ámbito. Trazabilidad de la ejecución presupuestaria interna (gastos operativos y contrataciones) y puntos de captura de evidencia ya existentes. Cada hito generará metadatos firmados, sellos de tiempo y huellas criptográficas con anclaje periódico en cadena pública; los documentos fuente y datos personales permanecerán off-chain con control de acceso (Ley 25.506, 2001; Ley 25.326, 2000).

(i) Denuncias e investigaciones → Evidencias y estados. Registro de radicación (fecha/hora, canal, tipología) y admisibilidad; apertura/inhibición de investigación preliminar; requerimientos a organismos; cierre o remisión (sede penal/querella). Cada actuación genera evento firmado y huella con anclaje por lote (Ley 25.188, 1999; OA, s. f.).

(ii) DDJJ (ARCA–AFIP) → Ciclo completo. Presentación (F.1245/F.1246), acuse ARCA, control de plazos (incl. prórrogas), y publicación de la porción accesible conforme la Ley 25.188; cada evento deja huella verificable (AFIP, s. f.; OA, 2025; Ley 25.188, 1999).

(iii) Registros de obsequios y viajes → Validación y publicación. Carga del acto, verificación por OA y publicación en el registro (dataset abierto); huellas de inclusión y pruebas de integridad para terceros (Decreto 1179/2016, 2016; OA, s. f.).

(iv) Ejecución presupuestaria/contrataciones → Rastro contable-documental. Compromiso/orden de compra, recepción/conformidad, factura/devengado y orden de pago/transferencia; en cada hito, hash + timestamp y prueba de inclusión verificables por AGN (externo) y SIGEN (interno), conforme Ley 24.156 (Ley 24.156, 1992).

Resultados esperados (criterios de salida). Cobertura ≥ 80 % de hitos con huellas verificables; calidad ≤ 5 % de divergencias on/off-chain en muestra auditada; oportunidad ≤ 24 h de latencia documento→anclaje (promedio mensual); aceptación de auditoría y del dueño del proceso (INTOSAI, 2013; OA, s. f.).

6.2 Etapas del despliegue

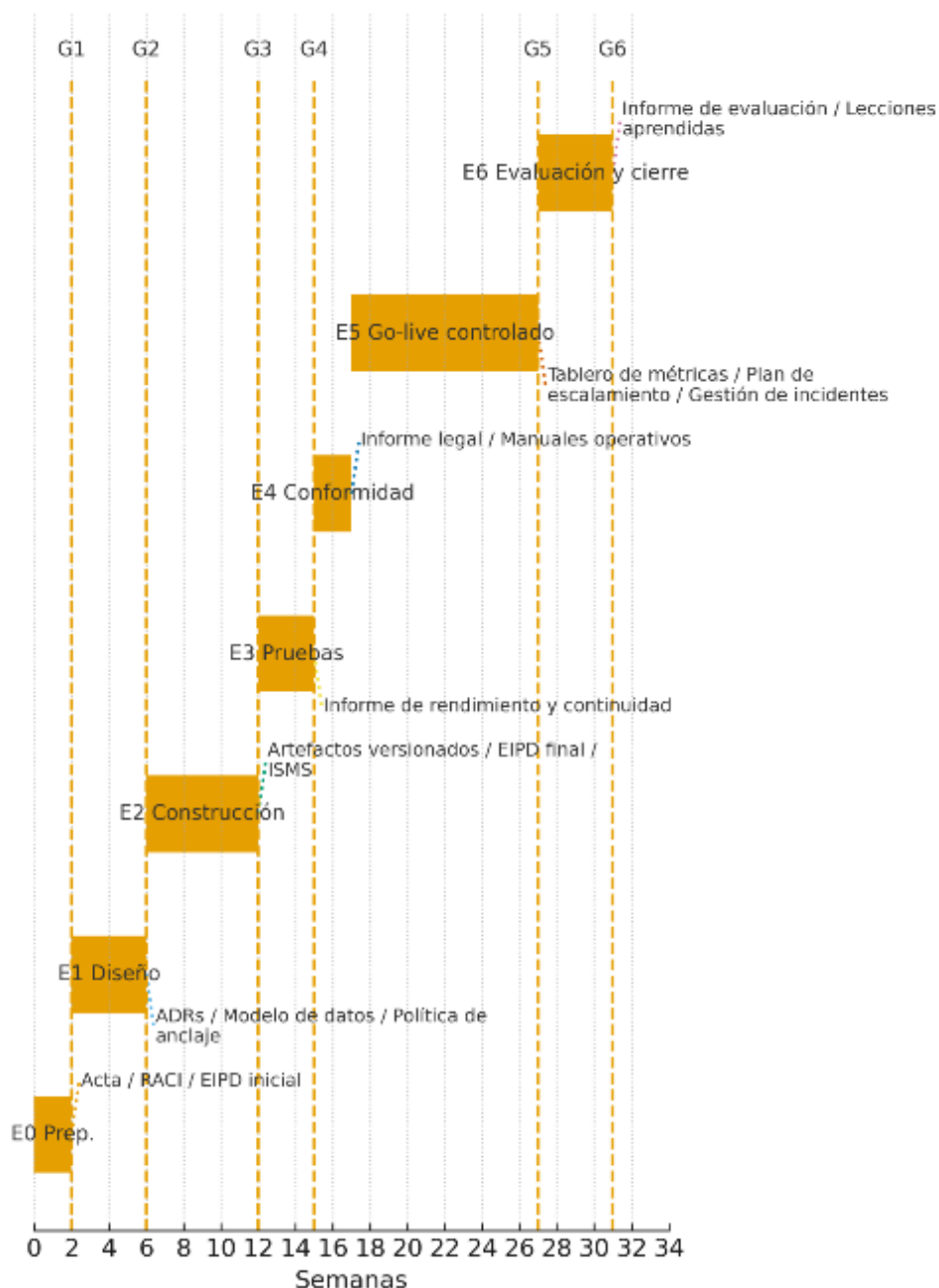
Visión general. El despliegue se organiza en seis etapas con gates de control (G1–G6). Cada etapa declara objetivos, actividades clave, responsables, riesgos y entregables verificables. El diseño integra privacidad por diseño y minimización de datos (AAIP & URCDP, 2020), controles de ciberseguridad basados en el NIST CSF (Identificar–Proteger–Detectar–Responder–Recuperar) (NIST, 2018), criterios de auditoría pública (INTOSAI, 2013) y lineamientos de auditoría de sistemas de gestión (ISO, 2018), bajo un ISMS conforme ISO/IEC 27001 (ISO/IEC, 2022) y medidas específicas de la AAIP Res. 47/2018 (AAIP, 2018). La publicación en cadena pública se rige por una política de anclaje multired (seguridad/latencia/costo), tomando como referencia las guías del Foro Económico Mundial & Banco Interamericano de Desarrollo para sector público (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020); los documentos fuente y datos personales permanecen off-chain con control de acceso (Ley 25.326, 2000). La Tabla 57 organiza el despliegue en etapas (E0–E6), con sus objetivos, gates de salida y principales entregables.

La Figura 63 presenta el roadmap del despliegue del piloto (E0–E6), con sus gates, duraciones estimadas y principales entregables.

Tabla 57*Etapas del despliegue, objetivos, gates y entregables (E0–E6)*

Etapa	Obj.	Act. clave	Gate	Entregables	Criterios
E0 (prep.)	Alinear alcances, riesgos y baseline (Fase 0).	Kickoff; baseline; RACI; EIPD inicial.	G1	Acta; plan; RACI; EIPD inicial.	Mandato/alcance aprobados; riesgos y supuestos documentados.
E1 Diseño (4s)	Definir arq./seg./controles; plan de pruebas.	ADRs; modelo de datos; política anclaje; matriz Controles↔Evid.	G2	ADRs; data model; política; plan de pruebas/aceptación.	Arq. aprobada; controles trazables a evidencia.
E2 Construcción (6s)	Contratos; ETL; integración/UI; observabilidad.	CI/CD; pruebas unit./est.; conectores; tablero verificación.	G3	Artefactos versionados; políticas; EIPD final; plan ISMS.	Cumpl. legal/seguridad; privacidad por diseño.
E3 Pruebas (3s)	Validar funcionalidad, seguridad, rendimiento y continuidad.	Carga/estrés; fallos de nodo; finalidad BFT; rastro; auditoría interna.	G4	Informe técnico; resultados rend./continuidad; criterios firmados.	p95 latencia y finalidad en objetivo; evidencia suficiente.
E4 Conformidad (2s)	Cierre legal/seguridad previo a operación controlada.	Dictamen legal; anexos; SoD; plan de publicación responsable.	G4→G5	Informe de pruebas; manuales; informe legal.	Criterios legales/operativos aprobados.
E5 Go-live ctrl. (8–12s)	Operar en paralelo (shadow) y medir con usuarios reales.	Go-live; anclaje multired; tablero; soporte; capacitación.	G5	Acta; tablero métricas; plan escalamiento; reporte incidentes.	T1–T3 en verde/ámbar; mesa de ayuda; 0 incidentes críticos.
E6 Eval./cierre (4s)	Medir resultados y decidir escalamiento/replacibilidad.	Eval. T1–T12; CBA/ROI; lecciones; roadmap expansión.	G6	Informe de evaluación; lecciones; plan de expansión; réplica.	Criterios §6.6.4 cumplidos o tendencia favorable.

Nota. Elaboración propia con base en los criterios y gates (G1–G6) y en los principios de medición reproducible. Abreviaturas: ADR = Architectural Decision Record; ISMS = Information Security Management System. Referencias de marco: INTOSAI (2013), ISO (2018), ISO/IEC (2022), NIST (2018) y Foro Económico Mundial & Banco Interamericano de Desarrollo (2020), AAIP (2018).

Figura 63*Roadmap del despliegue (E0–E6) con gates y entregables*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. Abreviaturas: ADR = Architectural Decision Record; EIPD = Evaluación de Impacto en Protección de Datos; ISMS = Information Security Management System; P95 = percentil 95. Las duraciones y gates representan el plan del piloto y pueden ajustarse según resultados de pruebas y criterios de salida.

E1. Preparación institucional — 4 semanas

Objetivo. Asegurar patrocinio, gobierno del proyecto y condiciones habilitantes (legales, organizacionales y técnicas).

Actividades clave.

Gobernanza y RACI: designación de sponsor, Comité de Pilotaje y responsables RACI (proceso, TI, legales/DPO, CISO, auditoría interna, enlaces SIGEN/AGN) (INTOSAI, 2013).

Alcance y caso de negocio: definir proceso, metas, supuestos, restricciones y métricas de éxito (COSO, 2013).

Cumplimiento y datos: clasificación de información, bases de legitimación, matriz de accesos y inicio de EIPD/DPIA (AAIP & URCDP, 2020).

Seguridad de la información: alineamiento a ISO/IEC 27001 y medidas AAIP Res. 47/2018; criterios de retención/borrado y segregación de funciones (ISO/IEC, 2022; AAIP, 2018).

Cambio y comunicación: mapa de stakeholders, plan de capacitación y comunicaciones (ISO, 2018).

Riesgos y tácticas. Déficit de patrocinio (acta formal + KPIs); subestimación de datos sensibles (EIPD temprana + talleres) (AAIP & URCDP, 2020).

Entregables. Acta de proyecto, plan de trabajo, matriz RACI, EIPD (borrador), política de anclaje híbrido (principios), plan de cambio. Gate G1: aprobación de Comité y conformidad DPO/legal (INTOSAI, 2013).

E2. Diseño detallado y conformidad — 4–6 semanas

Objetivo. Definir arquitectura, límites on/off-chain, contratos inteligentes, evidencias auditables y cerrar conformidades legal/seguridad.

Actividades clave.

Arquitectura lógica/física: protocolo permissionado (p. ej., Quorum/Besu o Hyperledger Fabric), identidad (PKI X.509), topología de nodos y borde on/off-chain (minimización, seudonimización) (ISO/IEC, 2022).

Política de anclaje multired: frecuencia (diaria en Ethereum; semanal en Bitcoin), merklización por lote, pruebas de inclusión (txid/altura) y criterios de costo/latencia (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Controles ↔ evidencias: mapeo de controles COSO/ISSAI y funciones NIST a eventos (alta/modificación/aprobación/anulación) y registros en contratos inteligentes (COSO, 2013; INTOSAI, 2013; NIST, 2018).

Seguridad y cumplimiento: modelo de amenazas; KMS/HSM para llaves; política de logs/monitoreo; EIPD final y anexo de medidas AAIP; trazabilidad legal (Ley 24.156, 1992; Ley 25.188, 1999; Ley 25.326, 2000; Ley 25.506, 2001).

Pruebas y aceptación: estrategia (unitarias, integración, seguridad, rendimiento, continuidad) y criterios de Definition of Done y aceptación por auditoría (ISO, 2018).

Riesgos y tácticas. Sobre-exposición de metadatos (agregación por lote y hash parciales); red inadecuada (matriz de decisión seguridad/latencia/costo) (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Entregables.ADRs, modelo de datos, BPMN, contratos inteligentes (borrador), matriz Controles↔Evidencias, plan de pruebas, EIPD final. Gates:G2 (arquitectura aprobada) y G3 (conformidad legal/seguridad cerrada) (ISO, 2018).

E3. Implementación del prototipo — 6–8 semanas

Objetivo. Construir un prototipo funcional con contratos inteligentes y conectores mínimos; preparar entornos y observabilidad.

Actividades clave.

Contratos inteligentes: reglas de compromiso, devengado, orden de compra, recepción y pago (segregación de funciones, umbrales, validación de firmas/duplicados) (COSO, 2013).

Integración mínima: conectores con ERP/contabilidad y portal de contrataciones (IDs de expediente/documento, metadatos) (Ley 24.156, 1992).

Infraestructura: nodos validadores/observadores; PKI institucional; KMS/HSM; canales/colecciones privadas si aplica (ISO/IEC, 2022).

Observabilidad: tableros de métricas (latencia documento→anclaje, cobertura de hitos con hash, divergencias on/off-chain), trazas y alertas (NIST, 2018).

Datos de prueba:dataset anonimizado con casos reales (muestreo estratificado) y evidencias de hash/sello temporal (AAIP & URCDP, 2020).

Riesgos y tácticas. Errores por manejo de llaves/roles (doble control y rotación); deuda técnica (reglas de calidad) (ISO/IEC, 2022).

Entregables.Prototipo funcional, entornos (dev/test/preprod), guías técnicas, dataset de prueba, tableros iniciales. Gate G4: pruebas técnicas de pre-aceptación superadas (ISO, 2018).

E4. Pruebas y validación — 4–6 semanas

Objetivo. Validar funcionalidad, seguridad, cumplimiento y auditabilidad del prototipo.

Actividades clave.

Pruebas técnicas: unitarias/integración; seguridad (autorización/segregación, fuzzing básico de contratos); rendimiento (picos y lotes); continuidad (RTO/RPO) (NIST, 2018; ISO/IEC, 2022).

Evidencia criptográfica: verificación de hashes, txid y alturas; pruebas de inclusión; revisión de divergencias on/off-chain (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Auditoría y conformidad: ejercicios de auditoría técnica (ISSAI 100) y auditoría de gestión (ISO 19011); revisión legal/DPO de publicación/anonimización y actualización de EIPD si corresponde (INTOSAI, 2013; ISO, 2018; AAIP & URCDP, 2020).

Capacitación y mesas de trabajo: talleres con auditoría (AGN/SIGEN) y con áreas legales/operativas para criterios de aceptación (INTOSAI, 2013).

Riesgos y tácticas. Rechazo por auditoría (co-diseño de evidencias y trazabilidad de papeles de trabajo); latencia excesiva (ajuste de lote/ventanas) (INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Entregables. Informe de pruebas, criterios de aceptación cumplidos, manuales operativos, informe legal de conformidad. Gates: G4 (aceptación técnica) y G5 (visto bueno legal/auditor) (ISO, 2018).

E5. Despliegue controlado — 8–12 semanas

Objetivo. Operar en modo paralelo (shadow) en una unidad y validar desempeño/uso con usuarios reales.

Actividades clave.

Go-live controlado: operación paralela con el circuito vigente; bitácoras y comparadores on/off-chain (NIST, 2018).

Anclaje multired: diario en Ethereum (latencia/visibilidad) y semanal en Bitcoin (resistencia a censura), según política de anclaje (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Tablero de verificación: consulta de huellas, cotejo on/off-chain y exportables para papeles de trabajo (INTOSAI, 2013).

Soporte y mejora: mesa de ayuda; observatorio de incidentes; sprints de ajuste (ISO/IEC, 2022).

Capacitación: sesiones a usuarios del proceso, auditoría y mesa de entradas (ISO, 2018).

Riesgos y tácticas. Incidentes operativos (plan de respuesta y reversión); sobredemanda de soporte (SLA, catálogo de servicios) (NIST, 2018).

Entregables. Acta de go-live, tablero de métricas, plan de escalamiento por fases, reporte de incidentes y mejoras. Gate G5: autorización para operación plena de la unidad (INTOSAI, 2013).

E6. Evaluación y cierre — 4 semanas

Objetivo. Medir resultados, consolidar lecciones y definir escalamiento/replicabilidad.

Actividades clave.

Evaluación de indicadores (ver §6.6): cobertura de hitos con hash (meta ≥ 80 %), divergencias on/off-chain (meta ≤ 5 %), latencia documento→anclaje (meta ≤ 24 h) y aceptación de auditoría (INTOSAI, 2013; NIST, 2018).

Análisis costo–beneficio y viabilidad de escalamiento OA-wide; estimación de OPEX/CAPEX y ROI (COSO, 2013).

Gestión del conocimiento:lecciones aprendidas, riesgos residuales y backlog para fase 2 (ISO, 2018).

Plan de expansión: roadmap interinstitucional con criterios de priorización y artefactos reutilizables (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Entregables.Informe de evaluación, lecciones aprendidas, plan de expansión, matriz de replicabilidad. Gate G6: cierre formal y decisión de escalamiento (ISO, 2018).

Puertas de salida (gates) y evidencia requerida.

G1 – Aprobación del proyecto: Acta, RACI, plan y EIPD inicial (AAIP & URCDP, 2020).

G2 – Aprobación de arquitectura: ADRs, modelo de datos, política de anclaje, matriz Controles↔Evidencias (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; NIST, 2018).

G3 – Conformidad legal/seguridad: EIPD final, anexo AAIP Res. 47/2018, trazabilidad legal (24.156/25.188/25.326/25.506), plan ISMS (AAIP, 2018; ISO/IEC, 2022).

G4 – Cierre de pruebas: informe técnico, rendimiento/continuidad, ejercicios de auditoría (ISSAI/ISO 19011), criterios de aceptación firmados (INTOSAI, 2013; ISO, 2018).

G5 – Go-live controlado: acta de puesta en marcha, tablero de métricas y mesa de ayuda activa (NIST, 2018).

G6 – Cierre: informe de evaluación, lecciones aprendidas y plan de expansión (ISO, 2018; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

6.3 Recursos humanos necesarios

Aquí se detalla la estructura del equipo, los perfiles y responsabilidades, la matriz RACI y el plan de dotación por fases (FTE) para ejecutar el piloto con segregación de funciones, control interno y aseguramiento independiente, en línea con buenas prácticas de auditoría y gestión de seguridad de la información (INTOSAI, 2013; ISO/IEC 27001:2022; ISO 19011:2018; COSO, 2013; NIST, 2018).

6.3.1 Estructura del equipo (núcleo del piloto)

Composición objetivo y dedicación estimada (FTE sobre la duración del piloto):

Dirección del proyecto – OA (0,5): responsable de alcance, riesgos, hitos y articulación con autoridades y órganos de control (SIGEN/AGN).

Arquitectura blockchain y seguridad (1,0): diseño de red permissionada, modelos de identidad/llaves, políticas de acceso y anclaje público; gestión de riesgos técnicos.

Desarrollo de contratos inteligentes (2,0): codificación, revisiones cruzadas, pruebas unitarias/estáticas, formalización de reglas de control.

Integración / full-stack (2,0): conectores con repositorios documentales/expedientes, APIs contables, UI de tablero de verificación.

DevOps / SRE (1,0): infraestructura como código, CI/CD, observabilidad, gestión de llaves/secretos, alta disponibilidad.

Ciencia de datos / ETL (1,0): normalización de metadatos, lotes de anclaje, calidad de datos y reconciliaciones on/off-chain.

Analista funcional contable-público (1,0): reglas contables y de contratación; mapeo de hitos a evidencias auditables.

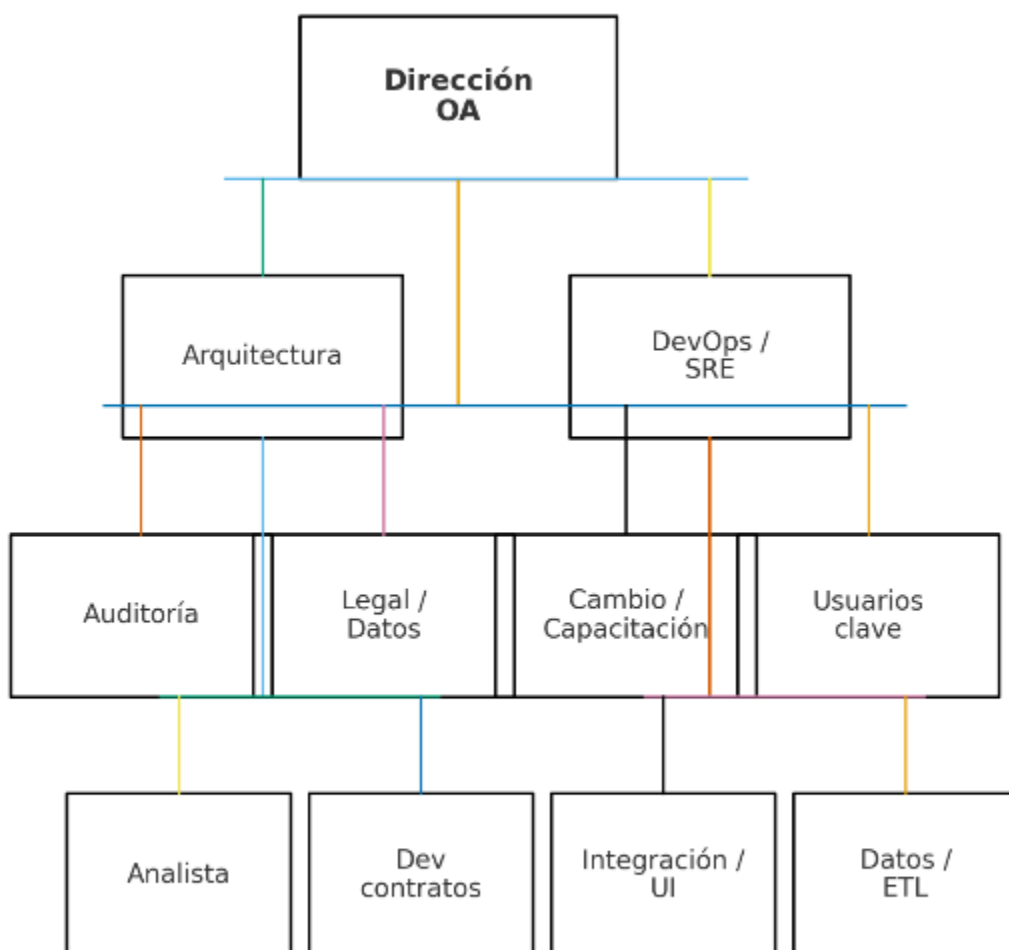
Auditoría interna / aseguramiento (0,5–1,0): pruebas de cumplimiento, revisión de suficiencia y apropiación de evidencias, independencia de línea (INTOSAI, 2013).

Asesoría legal y protección de datos (0,5): licitud del tratamiento, minimización, acuerdos de publicación selectiva y uso de firma/sello de tiempo.

Gestión del cambio y capacitación (0,5): adopción, manuales, guías de operación y acompañamiento a usuarios.

Dotación neta estimada: 10–11 FTE en promedio sobre el período del piloto. La auditoría y lo legal pueden operar en dedicación parcial con intensificación en hitos clave (INTOSAI, 2013; ISO 19011:2018).

Figura 64
Organigrama funcional



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. Dotación neta estimada: 10–11 FTE en promedio sobre el período del piloto. La auditoría y lo legal pueden operar en dedicación parcial con intensificación en hitos clave (INTOSAI, 2013; ISO 19011, 2018).

6.3.2 Responsabilidades y entregables por rol

Dirección del proyecto – OA: plan maestro, matriz de riesgos, actas de hito, gestión de stakeholders; entregables: Plan de Proyecto, Registro de Riesgos, Informe de Cierre.

Arquitectura blockchain y seguridad: arquitectura lógica/física, políticas de claves/roles, plan de hardening y continuidad; entregables: Documento Arquitectural, Matriz de Controles, DR/BCP (NIST, 2018; ISO/IEC 27001:2022).

Contratos inteligentes: especificaciones, código, pruebas unitarias, análisis estático y de gas; entregables: Especificación de Reglas, Repositorio Versionado, Resultados de Pruebas.

Integración / full-stack: APIs, adaptadores a sistemas fuente, UI del tablero, controles de integridad; entregables: Catálogo de APIs, Manual Técnico, Tablero funcional.

DevOps / SRE: pipelines CI/CD, monitoreo, logging, gestión de secretos, IaC; entregables: Pipelines, Tablero de Observabilidad, Runbooks.

Datos / ETL: diccionario de metadatos, mapeos origen→huella, validaciones y reconciliaciones; entregables: Diccionario & Esquemas, Jobs ETL, Informe de Calidad de Datos.

Analista funcional: BPMN “as-is/to-be”, criterios de aceptación, casos de prueba de negocio; entregables: Flujos y Casuística, Matriz de Requisitos, Evidencias de Aceptación.

Auditoría interna / aseguramiento: plan de auditoría del piloto, pruebas de suficiencia/propiedad de evidencia, management letter; entregables: Programa de Auditoría, Papeles de Trabajo, Informe de Aseguramiento (INTOSAI, 2013; ISO 19011:2018).

Legal / Datos personales: DPIA/EIPD, términos de publicación selectiva, políticas de retención; entregables: Informe Legal, DPIA/EIPD, Dictamen de Publicación.

Cambio y capacitación: plan de comunicaciones, guías y capacitaciones por rol; entregables: Plan de Adopción, Manuales (usuario/auditor/operador), Registro de Capacitaciones.

6.3.3 Matriz RACI (detallada)

Descubrimiento y priorización de requisitos: R Analista funcional · A Dirección OA · C Auditoría interna, Legal · I Equipo técnico.

Arquitectura y seguridad: R Arquitectura · A Dirección OA · C Legal, Auditoría · I Dev/DevOps (NIST, 2018; ISO/IEC 27001:2022).

Desarrollo de contratos inteligentes: R Dev contratos · A Dirección de proyecto · C Auditoría, Analista · I Legal.

Integración y UI: R Integración/full-stack · A Dirección de proyecto · C Analista, Seguridad · I Auditoría.

Datos/ETL y reconciliaciones: R Datos/ETL · A Dirección de proyecto · C Auditoría, Analista · I Seguridad.

DevOps/Infraestructura: R DevOps/SRE · A Dirección OA · C Seguridad, Auditoría · I Equipo dev.

Pruebas funcionales y de seguridad:R Analista + Seguridad · A Dirección de proyecto · C Auditoría · I Usuarios clave (ISO 19011:2018).

Aseguramiento / auditoría interna del piloto:R Auditoría interna · A Dirección OA · C Legal, Analista · I Equipo técnico (INTOSAI, 2013).

Cumplimiento legal y protección de datos:R Legal/Datos · A Dirección OA · C Seguridad, Auditoría · I Integración.

Gestión del cambio y capacitación:R Cambio/Capacitación · A Dirección OA · C Analista · I Todas las áreas.

Operación inicial y monitoreo:R DevOps/SRE · A Dirección OA · C Auditoría · I Usuarios.

En la tabla 58 a continuación se diagrama la matriz RACI.

Tabla 58*Matriz RACI detallada por actividad*

Actividad	Dir OA	Arq	SRE	Aud	Leg/Datos	Ana	DevC	Int/UI	ETL	Cambio	Usu
Descubrimiento/priorización	A			C	C	R					I
Arquitectura/securidad	A	R	I	C	C						
Dev. contratos inteligentes	A			C	I		R				
Integración/UI	A		I			C		R			I
Datos/ETL y reconc.	A		I	C		C			R		
DevOps/Infra	A		R	C	C						
Pruebas func./seg.	A			C		R					I
Aseguramiento/aud. int.	A			R	C	C					I
Cumpl. legal/datos	A	C	C	C	R						
Cambio/capacitación	A			C		C				R	I
Operación/monitoreo	A		R	C							I

Nota. Elaboración propia. Abreviaturas de roles: Dir OA = Dirección del proyecto – OA; Arq = Arquitectura blockchain y seguridad; SRE = DevOps/SRE; Aud = Auditoría interna; Leg/Datos = Asesoría legal y protección de datos; Ana = Analista funcional; DevC = Desarrollo de contratos; Int/UI = Integración y UI; ETL = Ciencia de datos/ETL; Cambio = Gestión del cambio y capacitación; Usu = Usuarios clave. Marcos de referencia: NIST (2018), ISO/IEC 27001 (2022), ISO 19011 (2018) e INTOSAI (2013).

6.3.4 Plan de dotación por fases (FTE y momentos de mayor carga)

La Tabla 59 resume la dotación estimada por fase del piloto, expresada en equivalentes de jornada completa (FTE), e identifica los picos de carga esperados. La distribución busca asegurar segregación de funciones y capacidad de aseguramiento independiente en los hitos críticos del proyecto.

Tabla 59

Plan de dotación por fases (FTE y picos de carga)

Fase	Dir OA	Arq	SRE	Aud	Leg/Datos	Ana	DevC	Int/UI	ETL	Cambio	Total FTE	Pico/sem
F0 Prep (2s)	0,5	1	0	0,5	0,5	1	0	0	0	0	3,5	3,5
F1 Diseño (4s)	0	1	0,5	0,5	0,5	1	0	0	0	0	3,5	3,5
F2 Constr. (6s)	0	0,5	1	0	0	0	2	2	1	0	6,5	6,5
F3 Pruebas (3s)	0	1	0,5	1	0,5	1	0	0	0,5	0	4,5	4,5
F4 Cierre (1s)	0,5	0	0,5	0,5	0	0	0	0	0	0,5	2	2

Nota. Elaboración propia. Abreviatura: FTE = Full-Time Equivalent. Los picos de carga se estiman como suma FTE por fase y se alinean con segregación de funciones y aseguramiento independiente (INTOSAI, 2013; ISO 19011, 2018).

Notas de gobernanza: a) mantener independencia del aseguramiento respecto del desarrollo (INTOSAI, 2013); b) preservar segregación de funciones (SoD) en operaciones clave y administración de llaves (ISO/IEC 27001:2022; COSO, 2013); c) documentar criterios de aceptación por rol (ISO 19011:2018).

6.3.5 Capacidades y plan de fortalecimiento

Técnicas: contratos inteligentes, criptografía aplicada, gestión de identidades/llaves, CI/CD, observabilidad, calidad de datos y reconciliaciones.

De control: diseño de evidencia suficiente y apropiada, traceability on/off-chain, controles preventivos/detectivos, papeles de trabajo (COSO, 2013; INTOSAI, 2013).

De cumplimiento: privacidad por diseño, DPIA/EIPD, publicación selectiva y retención (ISO/IEC 27001:2022).

Plan breve de formación (12–16 h): (i) fundamentos del piloto y responsabilidades; (ii) manejo del tablero de verificación; (iii) criterios de evidencia y pruebas de verificación; (iv) protocolos de incidentes y continuidad (NIST, 2018; ISO 19011:2018).

6.3.6 Indicadores de desempeño del equipo (KPIs)

Eficiencia: lead time requisito → despliegue, throughput de historias cerradas por sprint.

Calidad: tasa de defects críticos en producción, cobertura de pruebas, % de lotes de anclaje sin reproceso.

Seguridad: cumplimiento de controles (SoD, rotación de llaves, secrets hygiene), MTTR de incidentes.

Aseguramiento: % de evidencias calificadas como suficientes y apropiadas, hallazgos cerrados en plazo (INTOSAI, 2013; ISO 19011:2018).

6.4 Diagrama de Gantt de implementación

Con el propósito de dimensionar temporalmente la implementación de la propuesta, se presenta en este apartado un cronograma consolidado del piloto mediante un diagrama de Gantt. Su inclusión permite integrar en una sola representación la secuencia de actividades, los hitos de control, los responsables funcionales y el horizonte temporal estimado de ejecución. De este modo, el cronograma complementa lo desarrollado en los apartados previos sobre etapas del despliegue, recursos humanos y asignación de responsabilidades.

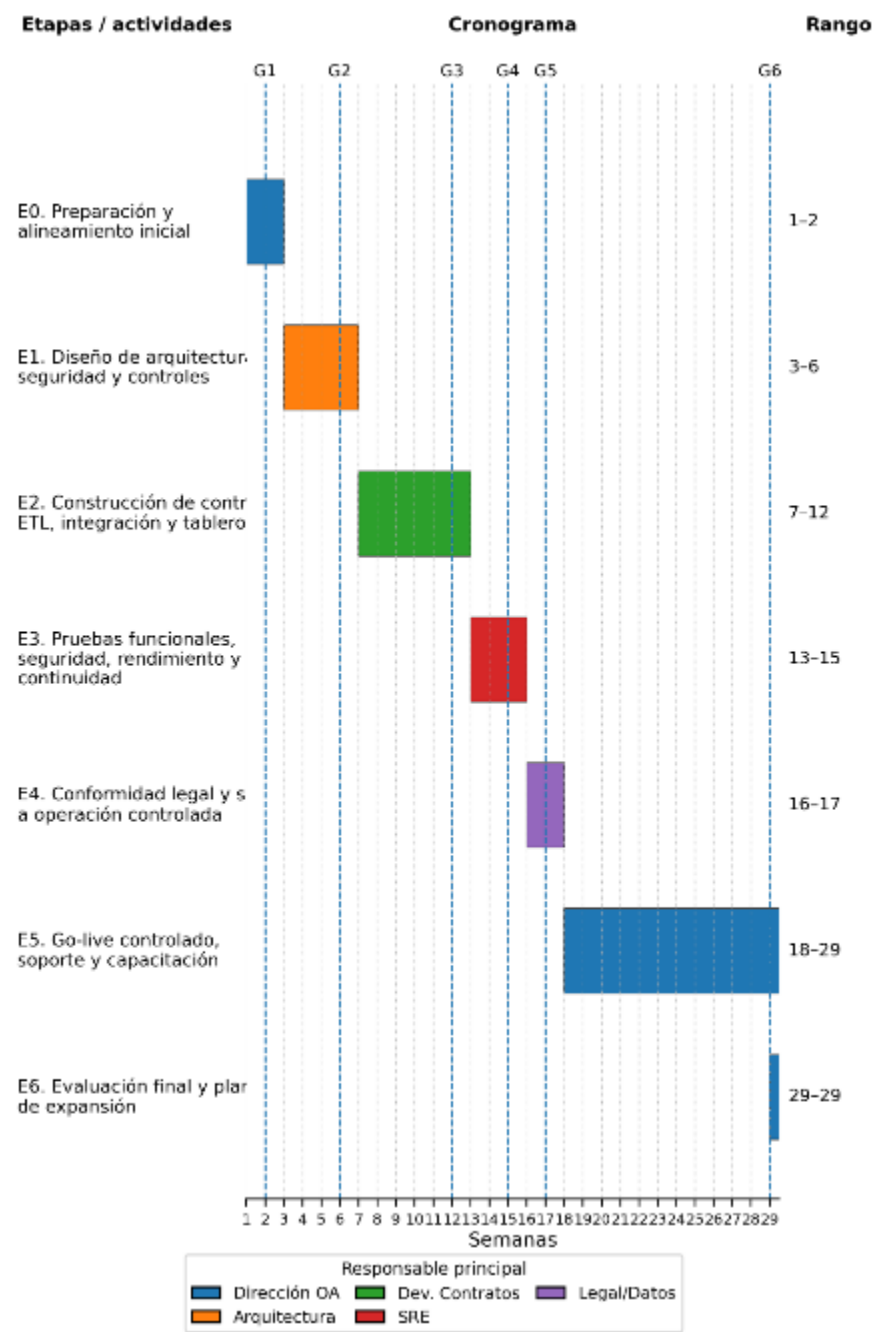
Desde una perspectiva de gestión, el diagrama permite traducir la arquitectura de implementación en una secuencia verificable de trabajo. En lugar de exponer por separado los recursos, los entregables y los momentos de control, el Gantt los articula en una vista única que facilita apreciar la lógica temporal del piloto, las dependencias entre etapas y la distribución del esfuerzo técnico y organizacional. Esta representación resulta especialmente pertinente en una propuesta de intervención, ya que permite mostrar no solo qué debe hacerse, sino también cuándo, con qué encadenamiento y bajo qué responsables.

El cronograma toma como base la hoja de ruta del despliegue estructurada en las etapas E0–E6 ya definidas en el trabajo. En ella se distinguen una fase inicial de preparación y alineamiento, una fase de diseño de arquitectura y controles, una etapa de construcción e integración, un tramo específico de pruebas, una instancia de conformidad jurídico-operativa previa a la salida controlada y, finalmente, una etapa de operación supervisada seguida de evaluación final y eventual expansión. Esta secuencia preserva la lógica gradual del proyecto y evita suponer una implementación lineal o inmediata.

Asimismo, el Gantt permite vincular el tiempo de ejecución con la dotación por fases y la distribución de responsabilidades ya especificadas en el capítulo. En ese sentido, fortalece la coherencia interna del plan de implementación, ya que las etapas del despliegue, la matriz RACI, la dotación por fase y el cronograma dejan de aparecer como elementos separados y pasan a conformar un esquema integrado de ejecución. La Figura 65 presenta de manera sintética el cronograma de implementación del piloto, integrando etapas, responsables funcionales, hitos y horizonte temporal estimado de ejecución.

A partir de la lectura del cronograma, puede observarse que la implementación se organiza como un proceso escalonado. La etapa inicial se orienta a la preparación institucional y la coordinación entre áreas; le siguen las fases de diseño y construcción, que concentran el mayor esfuerzo técnico; posteriormente, se prevén instancias de prueba y validación previas a la operación controlada; y, finalmente, una etapa de evaluación y cierre destinada a sistematizar resultados, lecciones aprendidas y criterios de replicabilidad.

Figura 65
Cronograma de implementación del piloto



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor sobre la base de las etapas del despliegue, la matriz RACI detallada por actividad y el plan de dotación por fases desarrollados en el capítulo 6.

6.5 Infraestructura tecnológica y costos

Esta sección presenta la arquitectura de referencia para el piloto de 12 meses, los principales supuestos de dimensionamiento y rendimiento, y una estimación referencial de costos (CAPEX/OPEX). El diseño se apoya en tres principios: (a) seguridad incorporada desde el diseño; (b) protección de datos personales mediante tratamiento mínimo y off chain; y (c) evidencia verificable por terceros mediante anclaje en cadena pública, en un esquema operativo sostenible (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; NIST, 2018; ISO/IEC, 2022; Ley 25.506, 2001; Ley 25.326, 2000).

6.5.1 Arquitectura de referencia

Capa permissionada (consorcio). La red principal es una blockchain permissionada operada por un consorcio de organismos públicos. Sus componentes clave son:

Red y consenso. Entre 3 y 5 nodos validadores con algoritmo tolerante a fallas bizantinas (p. ej., QBFT/PBFT), reglas claras de membresía, quórum y rotación de claves. Se añade un nodo observador de solo lectura, en red separada, para auditores y órganos de control, que permite verificación y replay de eventos sin privilegios de escritura (NIST, 2018; ISO/IEC, 2022).

Identidad y acceso. Gestión de identidades y accesos (IAM) basada en roles y atributos (RBAC/ABAC), autenticación multifactor para operaciones sensibles y diferenciación estricta entre cuentas humanas y de servicio.

Registro de evidencia. Libro de solo agregado (append-only) que encadena hashes y sellos de tiempo, almacenando solo metadatos necesarios y referencias a documentos off chain, conforme a minimización de datos (Ley 25.326, 2000).

API de verificación. Interfaces REST/gRPC para consultar huellas, pruebas de inclusión (árboles de Merkle) y metadatos firmados, con límites de uso y registro de accesos.

Capa pública (anclaje). Se utiliza exclusivamente para anclar evidencias en redes abiertas de alta disponibilidad:

Política multired. Anclaje diario en una red primaria (por ejemplo, Ethereum), semanal en una red secundaria (por ejemplo, Bitcoin) y mensual en una tercera red de respaldo. Cada operación publica un manifiesto con txid, altura de bloque, raíz de Merkle y algoritmo de hash, junto con reglas de reintento ante fallas o comisiones elevadas (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Batched anchoring. Los eventos del período se consolidan en una única raíz de Merkle por ventana, reduciendo costos y simplificando la verificación.

Servicios de confianza.

PKI y firma digital. Infraestructura de clave pública y firma digital conforme a la Ley 25.506, con sellado de tiempo confiable, sincronización de relojes (NTP/PTP redundante) y gestión de claves mediante KMS/HSM para custodia y rotación periódica (Ley 25.506, 2001; ISO/IEC, 2022).

Archivo y retención. Almacenamiento WORM/objeto con cifrado en reposo y políticas de retención y disposición final alineadas al régimen de datos personales (Ley 25.326, 2000).

Integración y datos.

Integración con sistemas fuente. Conectores con ERP/contabilidad y plataformas de contrataciones que generen metadatos sintéticos (ID de expediente, hito, actor, timestamp, hash del documento), aplicando minimización y, cuando corresponda, seudonimización (Ley 25.326, 2000).

Analítica. Data lake separado de la red de validación para analizar integridad (latencias, discrepancias on/off chain) sin impacto en el consenso.

Gestión y monitoreo.

Ciclo de vida y observabilidad. Uso de CI/CD, escaneo de vulnerabilidades, gestión de SBOM, telemetría (métricas, logs, trazas), alertas y tableros de salud con SLO/SLI definidos. Integración con SIEM para correlacionar eventos y soportar respuesta a incidentes (NIST, 2018; ISO/IEC, 2022).

Ambientes y segregación. Desarrollo, pruebas, preproducción y producción en dominios aislados, con datos enmascarados fuera de producción y segregación de funciones en administración, despliegue y operación (ISO/IEC, 2022).

6.5.2 Decisiones de diseño y supuestos

Las principales decisiones de diseño del piloto son:

Gestión de identidad y llaves. Claves de servicio administradas en HSM/KMS, rotación trimestral, mínimo privilegio y aprobación en modalidad de “cuatro ojos” para operaciones críticas (ISO/IEC, 2022).

Estrategia de anclaje. Ventanas configurables (por ejemplo, 24 horas), límites de comisión (fee cap) y colas de reintento. Si el costo supera el umbral, se activa fallback hacia la red secundaria.

Cada lote genera un manifiesto firmado apto para auditoría (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Privacidad incorporada al diseño. En la cadena solo se registran huellas y metadatos no identificatorios; documentos e identidades permanecen off chain, con controles de acceso, bitácoras y reglas de retención (Ley 25.326, 2000).

Continuidad operativa. Copias de seguridad verificadas, planes de recuperación ante desastres y continuidad del negocio, ensayos de restauración y objetivos RPO/RTO definidos para validadores, KMS y repositorios (NIST, 2018).

6.5.3 Dimensionamiento y rendimiento esperado (piloto 12 meses)

La Tabla 60 presenta los supuestos de dimensionamiento y rendimiento para el piloto de 12 meses, que sirven como base para estimar recursos técnicos, modelar desempeño y definir política de anclaje y recuperación.

Tabla 60

Supuestos de dimensionamiento y rendimiento del piloto (12 meses)

Aspecto	Supuesto
Volumen (12 m)	10k–30k hitos/año (20–60 × ~500 exp.)
Anclajes por red	Primaria: ~30–31/mes; Secundaria: 4–5/mes; Terciaria: 1/mes
Cómputo validadores	3–5 nodos; 4–8 vCPU; 16–32 GB RAM; 500 GB SSD; ≥1 Gbps
Servicios auxiliares	IAM/KMS/CI-CD/SIEM/logging 1–3 TB/año
Evidencias off-chain	0,1–0,5 TB/año (metadatos + manifiestos)
Latencia objetivo	≤24 h prom. mensual (P95 ≤36 h)
Tolerancia a fallas	5 validadores $f=1 \Rightarrow$ tolera 1 caída sin perder consenso

Nota. Elaboración propia con base en §6.4.2–§6.4.3. Abreviaturas: vCPU, RAM, SSD, KMS/HSM, ETL. Política de anclaje multired y ventanas de consolidación según diseño. (NIST, 2018; ISO/IEC, 2022; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Se proyecta un volumen anual de 10.000–30.000 hitos, ventanas diarias de anclaje y una infraestructura de 3–5 validadores con recursos moderados. La latencia documento → anclaje se sitúa en ≤ 24 horas en promedio mensual, compatible con cierres contables periódicos, y la red admite la caída de al menos un validador sin comprometer el consenso.

6.5.4 Estimación referencial de costos (capex/opex)

La estimación se circunscribe a infraestructura y operación técnica; el costo del equipo humano se detalla en §6.3. Los valores se expresan en rangos mensuales en USD para un piloto de 12 meses y son orientativos, sujetos a modalidad de contratación, tipo de nube o centro de datos y reutilización de servicios existentes.

Tabla 61

Estimación referencial de costos (CAPEX/OPEX) por rubro

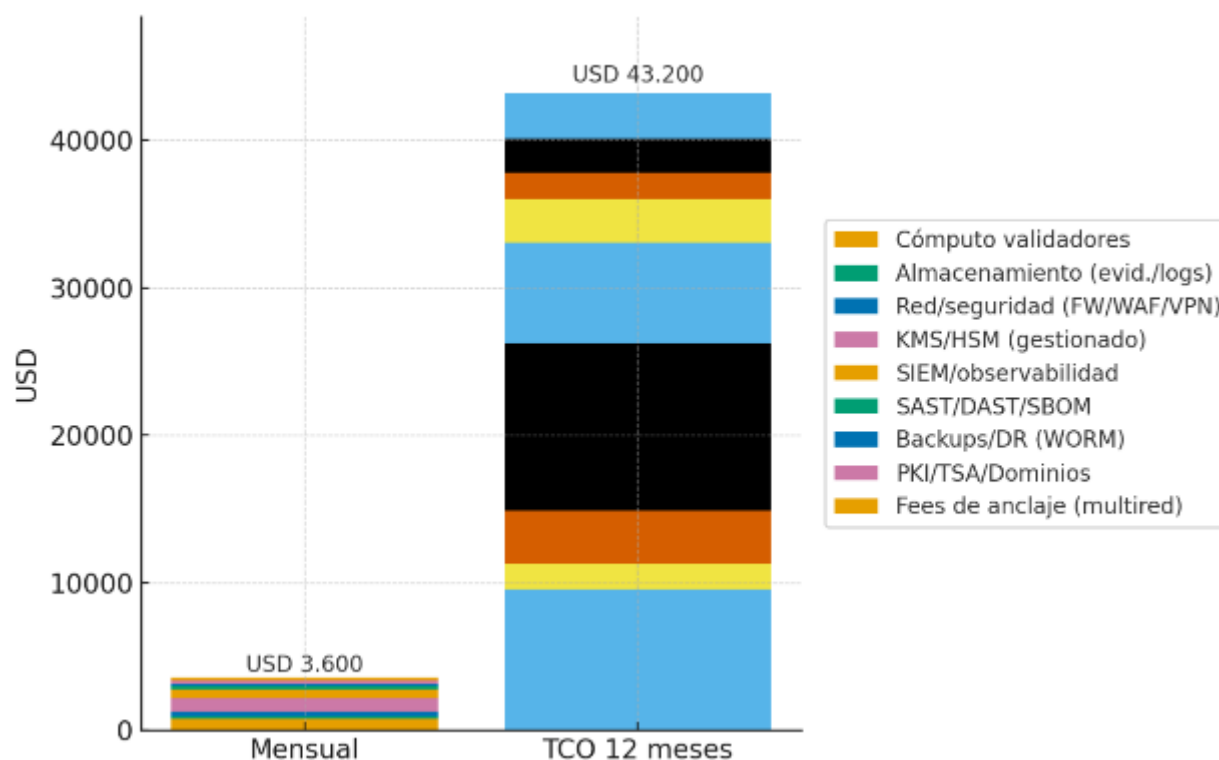
Rubro	Rango/mes	Supuesto	Política
Cómputo validadores	USD 600–1.500	5–7 VM/hosts	Dimensionamiento/SLAs
Alm. evidencias/logs	USD 80–300	1–3 TB/año	Retención
Red/seg. (FW/WAF/VPN)	USD 200–600	Perfil exposición	Monitoreo/SLA
KMS/HSM (gest.)	USD 500–2.000	Slots/throughput	Política de llaves
SIEM/observab.	USD 300–1.200	Volumen de logs	Gobierno eventos
SAST/DAST/SBOM	USD 150–500	Cobertura análisis	Ciclo seguro
Backups/DR (WORM)	USD 100–300	RPO/RTO	Pruebas trimestrales
PKI/TSA/Dominios	USD 100–400	Si no estatal	Trazabilidad sellos
Fees anclaje (multired)	USD 80–600	Batch/fee-cap/ventanas	Techo anual
Subtotal mensual (med.)	USD 3.000–4.000		
TCO 12 meses (ref.)	USD 36.000–48.000		

Nota. Elaboración propia con base en §6.4.4 (escenario piloto 12 meses; rangos orientativos en USD; no incluye costo de equipo humano, ver §6.3). Abreviaturas: CAPEX/OPEX, SIEM, SAST/DAST/SBOM, WORM, PKI/TSA. Política de fee-cap y batching para anclaje. (NIST, 2018; ISO/IEC, 2022; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La Figura 66 ilustra de forma sintética la distribución referencial entre CAPEX, OPEX y fees de anclaje.

Figura 66

Balance de costos: CAPEX/OPEX y fees de anclaje (escenario piloto).



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. Rubros incluidos: cómputo de validadores, almacenamiento de evidencias/logs, red/seguridad (FW/WAF/VPN), KMS/HSM, SIEM/observabilidad, SAST/DAST/SBOM, backups/DR, PKI/TSA y fees de anclaje. “Mensual” refleja un escenario medio normalizado a ~USD 3.600; “TCO 12 meses” corresponde a ~USD 43.200 (orientativo).

En términos agregados, pueden definirse tres escenarios técnicos: contenido (~USD 1.800/mes), medio (~USD 3.000–4.000/mes) y robusto/gestionado (~USD 5.000–6.500/mes), según intensidad de servicios gestionados y ventanas de retención. Los ahorros potenciales provienen de batching y elección de ventanas de anclaje, reutilización de servicios institucionales (PKI/TSA, observabilidad), segmentación de retención (hot/warm/cold) y uso de infraestructura como código.

No obstante, la viabilidad económica del piloto no debería evaluarse exclusivamente a partir del costo inicial o de la estimación correspondiente a una primera etapa de implementación. En términos institucionales, la sostenibilidad de la propuesta depende también de la capacidad de absorber costos recurrentes asociados al mantenimiento evolutivo y correctivo, al monitoreo continuo de la plataforma, a la actualización de componentes, a la seguridad operativa, a la custodia de claves, a la observabilidad de la infraestructura y a la capacitación periódica de los equipos involucrados. En consecuencia, el costo de mantenimiento en el tiempo no constituye un aspecto accesorio, sino una condición estructural para la continuidad de la solución, especialmente en organismos públicos sujetos a restricciones presupuestarias, ciclos administrativos anuales y reordenamientos de prioridades.

Finalmente, un piloto técnicamente satisfactorio no garantiza, por sí mismo, su escalamiento institucional, si no existe una previsión presupuestaria de mediano plazo que permita sostener su operación, su soporte y su mejora continua.

6.5.5 Riesgos técnicos y mitigaciones

La arquitectura híbrida concentra inversión en la capa permitida (control de acceso, trazabilidad y resiliencia) y utiliza el anclaje público como prueba de existencia de bajo volumen y alta verificabilidad, lo que estabiliza costos y facilita auditoría independiente sin exponer datos personales (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; Ley 25.326, 2000). Los principales riesgos técnicos y sus mitigaciones son:

Picos de comisiones en redes públicas. Umbrales de comisión (fee cap), colas de reintento y estrategia multired con fallback; monitoreo de comisiones y uso de ventanas fuera de picos (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Compromiso o mala gestión de claves. Uso de HSM/KMS, rotación periódica, controles de cuatro ojos, segregación de funciones y accesos just-in-time, alineados con buenas prácticas de seguridad (ISO/IEC, 2022).

Derivas de configuración y seguridad. Políticas de hardening, benchmarks (p. ej., CIS), escaneo continuo y pipelines de CI/CD con controles de seguridad integrados (NIST, 2018).

Desincronización temporal. Fuentes de tiempo redundantes (NTP/PTP), verificaciones cruzadas de sellos de tiempo y alertas por desvíos.

Crecimiento de volumen. Escalado horizontal de validadores y procesos ETL, segmentación de colas y mecanismos de backpressure en los pipelines.

En conjunto, el diseño permite controlar superficie de ataque, contener costos y mantener la evidencia accesible para auditoría interna, externa y social, manteniendo el contenido identificable fuera de la cadena.

6.6 Aspectos legales y regulatorios

Validez probatoria y firma digital. Los documentos electrónicos del piloto —actos administrativos, asientos, manifiestos de anclaje y evidencias— contarán con firma digital y sellado de tiempo dentro de la Infraestructura de Firma Digital (IFD), lo que les otorga idéntica eficacia y valor probatorio que sus equivalentes en soporte papel, siempre que se cumpla la Ley 25.506 y su reglamentación (Ley 25.506, 2001; Decreto 182/2019). La gestión electrónica de expedientes y trámites oficiales (p. ej., GDE/TAD) refuerza la interoperabilidad y la trazabilidad de actuaciones (Decreto 561/2016; Decreto 1063/2016). Cada manifiesto de anclaje incluirá metadatos mínimos (algoritmo, raíz Merkle, txid, altura de bloque, ventana temporal), firma digital y sello de tiempo, mientras que la cadena de custodia se asegura con KMS/HSM, rotación periódica de claves y controles de doble intervención (INTOSAI, 2013).

Ética pública e integridad. El diseño se alinea con los deberes y prohibiciones de la Ley 25.188 (conflictos de intereses, transparencia activa, rendición de cuentas) y aporta evidencia objetiva para prevenir, detectar y sancionar desvíos de conducta. En paralelo, la trazabilidad verificable facilita acreditar programas de integridad de personas jurídicas y mecanismos de control, en línea con la Ley 27.401 y su Decreto 277/2018 (Ley 25.188, 1999; Ley 27.401, 2017; Decreto 277/2018).

Protección de datos y acceso a la información. Se aplica privacidad por diseño y por defecto: minimización, seudonimización/anonimización y publicación selectiva; los datos personales y documentos fuente permanecen off-chain con control de acceso y bitácoras, mientras que on-chain solo se publican huellas y metadatos no identificatorios, con esquemas de retención y disposición final definidos (Ley 25.326, 2000; Decreto 1558/2001; AAIP, 2018). Para tratamientos de mayor riesgo se ejecutará una Evaluación de Impacto en la Protección de Datos (EIPD/DPIA) siguiendo la guía de AAIP–URCDP (AAIP & URCDP, 2020). La transparencia activa y las solicitudes de acceso se rigen por la Ley 27.275, aplicando el test de daño y las excepciones legales para resguardar datos personales y secretos protegidos; se clasificarán los datos como públicos, restringidos o confidenciales con reglas explícitas de publicación (Ley 27.275, 2016).

Contrataciones públicas y trazabilidad. La notaría de eventos licitatorios (pliegos, aclaraciones, actas de apertura, dictámenes, adjudicación, órdenes de compra, recepción/conformidad y pagos) refuerza la exigencia de trazabilidad del Régimen de Contrataciones y su Reglamento y mejora la auditabilidad frente a control interno (SIGEN) y externo (AGN), en el marco de la Ley 24.156 (Decreto 1023/2001; Decreto 1030/2016; Ley 24.156, 1992).

Gobernanza y responsabilidades. Un Comité de Gobernanza (OA + control interno + asesoría legal + seguridad de la información) aprobará políticas de acceso y publicación selectiva, plan de gestión de incidentes (detección, respuesta, notificación y remediación), criterios de revocación/rotación de llaves y programas de auditoría periódica. La segregación de funciones (SoD) y el aseguramiento independiente se alinean con COSO e ISSAI/INTOSAI, garantizando evidencia suficiente y apropiada y trazabilidad del control (COSO, 2013; INTOSAI, 2013).

Riesgos legales y mitigaciones. (i) Exposición de datos personales → on/off-chain por diseño, minimización/seudonimización, EIPD y controles de acceso (Ley 25.326, 2000; AAIP, 2018); (ii) nulidades por defectos formales de firma/sello → certificados válidos, TSA oficial, doble verificación de cadena de confianza y sellos a nivel evidencia/manifiesto (Ley 25.506, 2001; Decreto 182/2019); (iii) impugnaciones en contratación → registro inmutable de hitos, pruebas de inclusión y versionado disponible para auditoría (Decreto 1023/2001; Decreto 1030/2016); (iv) tensiones entre transparencia y confidencialidad → test de daño, clasificación de datos y publicación selectiva (Ley 27.275, 2016; Ley 25.326, 2000).

6.6 Indicadores e instrumentos de medición

En esta sección se definen los indicadores que se emplearán para seguir el desempeño del piloto, junto con su forma de cálculo, frecuencia de medición y fuentes. Se busca que los indicadores sean específicos, medibles y auditables, con trazabilidad de datos y posibilidad de reproducción independiente de los resultados. El enfoque se alinea con el criterio de evidencia suficiente y apropiada (INTOSAI, 2013), con las prácticas de control y auditoría de sistemas (ISO, 2018; ISO/IEC 27001:2022) y con la gestión del riesgo operativo (NIST, 2018). Metodológicamente, se prevé una línea de base previa al piloto, seguimiento mensual y evaluación pre/post con muestreo y herramientas de investigación social (Hernández et al., 2022).

6.6.1 Definiciones operacionales y metas

Eficiencia y control
T1. Tiempo medio de auditoría de transacciones críticas (días).

Definición: número de días hábiles entre la selección de la muestra y el cierre del procedimiento de auditoría.

Fórmula:

$$\bar{t} = \frac{1}{n} \sum_{i=1}^n (t_{\text{cierre},i} - t_{\text{inicio},i})$$

Frecuencia: mensual (promedio y P90).

Meta: -30 % respecto de la línea de base al mes 6 y -40 % al mes 12 (ISO, 2018; INTOSAI, 2013).

T2. Porcentaje de eventos con anclaje verificado y evidencia íntegra (%).

Definición: proporción de eventos en los que el hash recalculado coincide con la raíz de Merkle y el txid publicados, con sello temporal dentro de la ventana de servicio acordada.

Fórmula:

$$\frac{\text{\#eventos verificados}}{\text{\#eventos totales}} \times 100$$

Meta: ≥ 97 % mensual y ≥ 99 % trimestral (NIST, 2018).

T3. Latencia de registro y disponibilidad del servicio (SLA).

Definición: tiempo documento $\rightarrow$ anclaje (P95) y disponibilidad de APIs/nodos.

Metas: latencia ≤ 24 h de promedio mensual ($P95 \leq 36$ h) y disponibilidad $\geq 99,5$ % (NIST, 2018).

T4. Disminución de observaciones por falta de evidencia (variación %).

Definición: variación interanual de hallazgos u observaciones por evidencia insuficiente en auditorías internas y externas.

Fórmula:

$$\frac{\text{obs}_t - \text{obs}_0}{\text{obs}_0} \times 100$$

Meta: ≤ -40 % al mes 12 (INTOSAI, 2013).

Transparencia y trazabilidad

T5. Procesos licitatorios con rastro completo en cadena (%).

Definición: porcentaje de licitaciones en las que todos los hitos relevantes están notarizados (pliego, aclaraciones, apertura, dictamen, adjudicación, orden, recepción, pago).

Meta: ≥ 85 % al mes 6 y ≥ 95 % al mes 12 (ISO, 2018).

T6. Divergencias entre libros internos y estado en blockchain (%).

Definición: discrepancias sustantivas entre asientos/estados off-chain y huellas on-chain identificadas en las reconciliaciones.

Meta: ≤ 1 % mensual y 0 % de discrepancias críticas (INTOSAI, 2013).

T7. Cobertura de publicación activa (datasets y metadatos adecuados).

Definición: porcentaje de datasets comprometidos en el plan de transparencia que cuentan con metadatos completos (responsable, frecuencia, diccionario, versión).

Meta: 100 % de los compromisos trimestrales (ISO, 2018).

Seguridad y cumplimiento

T8. Incidentes de integridad/accesos no autorizados/reintentos de anclaje (conteo y severidad).

Definición: número de eventos clasificados por severidad (crítico, alto, medio) según el procedimiento de respuesta.

Metas: 0 incidentes críticos, ≤ 2 incidentes altos por mes y reintentos de anclaje $\leq 5\%$ (NIST, 2018; ISO/IEC 27001:2022).

T9. Conformidad con controles COSO/ISSAI (índice 0-100).

Definición: índice ponderado que resume el grado de cumplimiento de los componentes de control interno (ambiente, evaluación de riesgo, actividades de control, información/comunicación, monitoreo) y de los criterios ISSAI sobre evidencia.

Meta: $\geq 85/100$ sostenido y mejora de al menos 10 puntos porcentuales respecto de la línea de base (COSO, 2013; INTOSAI, 2013).

T10. Resultados de pruebas de continuidad (RTO/RPO efectivo).

Definición: porcentaje de ejercicios de continuidad en los que el RTO/RPO medido cumple con los objetivos definidos en el plan.

Meta: $\geq 95\%$ de las pruebas dentro de objetivo y sin fallas críticas recurrentes (ISO, 2018; NIST, 2018).

Adopción y satisfacción

T11. Satisfacción de auditores/usuarios (Likert 1–5).

Definición: promedio ponderado de ítems sobre facilidad de uso, confianza en la evidencia, utilidad de tableros y soporte.

Meta: $\geq 4,2/5$ con intervalo de confianza del 95 % y tasa de respuesta $\geq 60\%$ (Hernández et al., 2022).

T12. Personal clave capacitado y certificado (%).

Definición: proporción de usuarios críticos que completan la capacitación y superan una evaluación con más del 80 % de respuestas correctas.

Meta: $\geq 90\%$ al mes 3 y 100 % al mes 6 (ISO, 2018).

Los indicadores T1–T12 se interpretarán con una escala de colores RAG: verde cuando se cumple la meta o el intervalo de confianza resulta favorable; ámbar si el valor se encuentra a menos del 10 % de la meta o se observa tendencia negativa durante dos meses; rojo si el desvío supera el 10 % o se asocia a un incidente crítico (NIST, 2018; INTOSAI, 2013). Sobre esta base, la Tabla 62 sistematiza las definiciones operacionales de los indicadores T1–T12, sus metas asociadas y los responsables de su seguimiento. El objetivo es vincular cada métrica con una fuente de datos, un criterio de aceptación y un esquema de gobierno que permita interpretar de forma homogénea el tablero técnico del piloto.

Tabla 62*Definiciones operacionales de indicadores (T1–T12), metas y gobierno*

Cod	Nombre	Fórmula	Base	Meta	Freq	Fuente	Resp	Aseg.
T1	Tiempo medio de auditoría (días)	Prom. días háb. inicio→cierre	Base	–30% m6; –40% m12	Mens.	Papeles; bitácora	Dir OA	Aud. (val.)
T2	Eventos con anclaje verificado (%)	# verificados/# totales ×100	Base	≥97% m; ≥99% t	M/Trim	Logs; manifestos	Seg/SRE	Rastro (aud.)
T3	Latencia doc→anclaje (P95) y uptime	P95 y disponibilidad (%)	Base	P95 ≤36 h; ≥99,5%	Mens.	Telemetría; APIs	Seg/SRE	Control charts
T4	Obs. por falta de evidencia (var. %)	$(\text{obs_t} - \text{obs_0}) / \text{obs_0} \times 100$	Base	≤ –40% m12	M/Anual	Informes aud.	Dir OA	Aseg. ind.
T5	Licitaciones con rastro completo (%)	% con todos los hitos notarizados	Base	≥85% m6; ≥95% m12	M/Trim	Expediente; manif.	Compras/Transp.	Muestreo
T6	Divergencias on/off-chain (%)	% discrepancias relevantes	Base	≤1% m; 0% críticas	Mens.	Reconc. ETL	Contab/Aud.	Reconc. ind.
T7	Cobertura publicación activa (%)	% datasets con metadatos adecuados	Base	100% compromisos	Trim	Portal + plan	Transparencia	Rev. Legal/Datos
T8	Incidentes / reintentos de anclaje	Conteo y severidad	Base	0 críticos; ≤2 altos/mes; ≤5% reint.	Mens.	SIEM; incidentes	Seg/SRE	Post-mortems
T9	Índice conformidad COSO/ISSAI (0–100)	Puntaje ponderado	Base	≥85/100 y +10 p.p.	Trim	Checklists; aud. sist.	Auditoría	Comité control
T10	Pruebas de continuidad (RTO/RPO)	% ejercicios que cumplen	Base	≥95% cumplen; 0 fallas repet.	Trim	Actas; tiempos	Seg/SRE	Aud. continuidad
T11	Satisfacción usuarios/aud. (1–5)	Prom. ponderado (IC95%)	Base	≥4,2/5; resp. ≥60%	Trim	Encuestas	Cambio/Cap.	Calidad instrum.
T12	Personal crítico certificado (%)	% con >80% evaluación	Base	≥90% m3; 100% m6	Mens.	Registro capacit.	Cambio/Cap.	Verif. aud.

Nota. Elaboración propia. Los indicadores T1–T12 se interpretan con una escala RAG (Rojo/Ámbar/Verde) y se alinean con criterios de monitoreo continuo y suficiencia de evidencia propuestos en NIST (2018) e INTOSAI (2013).

6.6.2 Instrumentos y método de medición

Tablero de métricas con series y alertas. Consolida telemetría, logs de anclaje/ETL, estados de auditoría y disponibilidad de servicios; calcula P50/P90/P95 y aplica gráficos de control para distinguir variación común de variación especial (NIST, 2018).

Checklists de evidencia suficiente y apropiada. Listas normalizadas que permiten verificar existencia, integridad, trazabilidad y oportunidad de cada hito documentado (INTOSAI, 2013).

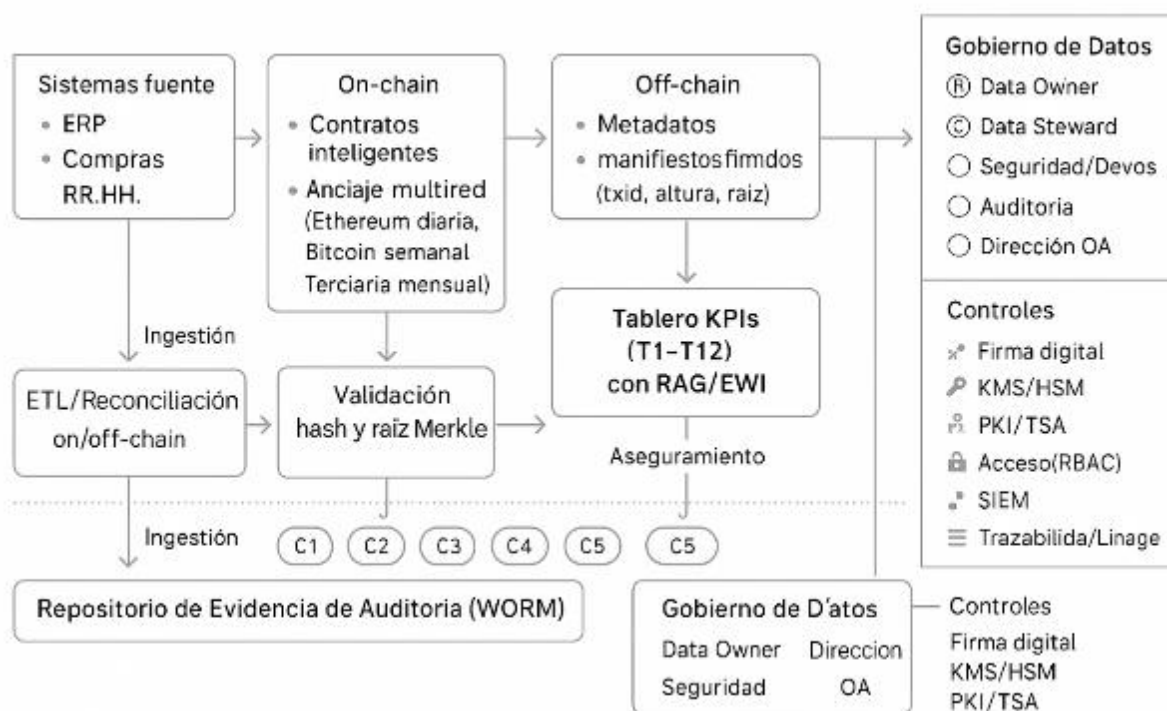
Muestreo estadístico estratificado. Muestreo por tipo de proceso, monto o criticidad y etapa; el tamaño muestral se calcula con IC 95 % y margen de error ≤ 5 %, documentando los pasos para asegurar la replicabilidad (INTOSAI, 2013; ISO, 2018).

Recreación del rastro. Pruebas de verificación de hash y txid, inclusión en árboles de Merkle, cotejo on/off-chain y recálculo independiente.

Encuestas y grupos focales. Cuestionarios tipo Likert validados, con prueba piloto de ítems, control de sesgos y análisis de confiabilidad (por ejemplo, α de Cronbach) (Hernández et al., 2022).

Pruebas de continuidad. Simulacros de restauración, rotación de llaves y fallas de anclaje, con actas y tiempos cronometrados (ISO, 2018; NIST, 2018).

La Figura 67 resume la arquitectura de medición y aseguramiento de KPIs: desde la ingesta de datos en sistemas fuente hasta el depósito WORM de evidencias, pasando por el registro on-chain, las evidencias off-chain, los procesos de ETL y reconciliación, la validación de hashes y raíces de Merkle, el tablero de indicadores con semaforización RAG y las funciones de Gobierno de Datos (Data Owner, Data Steward, Seguridad/DevOps, Auditoría y Dirección OA) que aplican controles criptográficos, de acceso y de trazabilidad (INTOSAI, 2013; ISO/IEC 27001:2022; NIST, 2018; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Figura 67*Arquitectura de medición y aseguramiento de KPIs*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en la política de anclaje y aseguramiento definida (INTOSAI, 2013; ISO/IEC 27001, 2022; NIST, 2018; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

6.6.3 Gobierno de la medición y aseguramiento

Propietarios de métrica. Dirección OA para T1–T4; Compras y Contabilidad para T5–T6; Seguridad/DevOps para T3 y T8–T10; área de Transparencia para T7; Auditoría como responsable de validación cruzada de T2, T5–T6 y T9.

Cadencia. Corte mensual con revisión trimestral; hitos específicos en pre-piloto (línea de base), mitad del piloto (mes 6) y cierre (mes 12).

Calidad de datos. Reglas de integridad, trazabilidad de cálculos, versionado de definiciones y auditoría independiente de métricas para asegurar que la información sea adecuada para tomar decisiones (INTOSAI, 2013; ISO, 2018).

Reporte y decisiones. Tablero con codificación RAG y explicación de causa raíz para los desvíos; planes de acción con responsables y plazos; y decisiones de go/no-go al cierre del piloto según el desempeño agregado.

6.6.4 Criterios de éxito

Eficiencia y control. T1 con reducciones de -30% al mes 6 y -40% al mes 12; T2 por encima de $97-99\%$; T3 con disponibilidad $\geq 99,5\%$ y $P95 \leq 36$ h; T4 con reducción $\geq 40\%$ de observaciones por falta de evidencia.

Transparencia y trazabilidad. T5 por encima del 95% al mes 12; $T6 \leq 1\%$ de discrepancias relevantes y 0% críticas; T7 con 100% de datasets comprometidos publicados con metadatos adecuados.

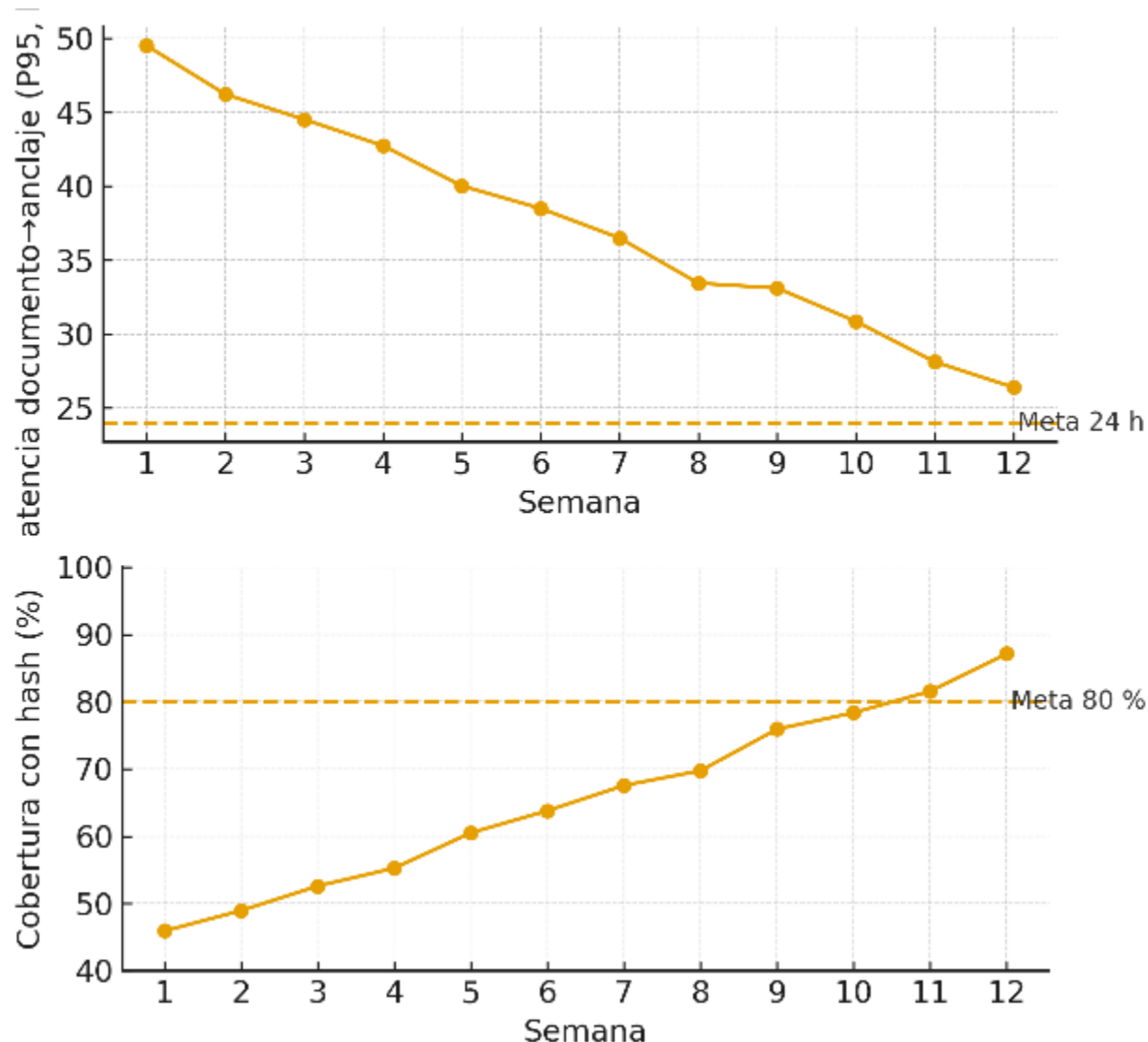
Seguridad y cumplimiento. T8 sin incidentes críticos; T9 con índice $\geq 85/100$; T10 con al menos el 95% de las pruebas de continuidad dentro de los objetivos.

Adopción y satisfacción. T11 $\geq 4,2/5$ con IC 95% ; T12 con el 100% del personal crítico capacitado y certificado en los plazos previstos.

La Figura 68 presenta, de manera comparativa, la evolución de la latencia documento→anclaje y de la cobertura con hash frente a las metas definidas. Este seguimiento permite identificar desvíos tempranos en desempeño y completitud de evidencias, y ajustar parámetros operativos antes de afectar cierres contables o auditorías.

Figura 68

Latencia documento→anclaje y cobertura con hash (metas vs. línea base).



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en metas y seguimiento operativo. Abreviaturas: P95 = percentil 95; Uptime = disponibilidad; Cobertura con hash = proporción de eventos con huella criptográfica verificada. Los valores son ilustrativos para el diseño de la figura y deben reemplazarse por la serie real del tablero operativo.

6.7 Gestión del cambio y capacitación

Esta sección establece cómo se prepara a las personas, cómo se comunica el propósito y cómo se sostiene la adopción del piloto en operación real. El enfoque combina principios de gestión del cambio (alineación, compromiso, refuerzo), pedagogía basada en competencias y mejora continua guiada por

métricas (Kotter, 2012; Hiatt, 2006; INTOSAI, 2013; ISO, 2018; ISO/IEC 27001:2022; NIST, 2018; Hernández et al., 2022).

6.7.1 Objetivos y principios

Objetivo general. Lograr adopción segura, medible y sostenible del piloto, minimizando fricción operativa e incrementando la confianza en la evidencia (INTOSAI, 2013; NIST, 2018).

Principios. (i) Comunicación temprana y frecuente con mensaje de propósito público (integridad, trazabilidad, rendición de cuentas); (ii) aprendizaje por casos reales y práctica supervisada; (iii) privacidad y seguridad por diseño en cada material/actividad; (iv) refuerzo con métricas de adopción y acompañamiento en el puesto; (v) liderazgo visible y patrocinio ejecutivo (Kotter, 2012; ISO/IEC 27001:2022).

6.7.2 Comunicación y acompañamiento operativo

Narrativa de cambio (“por qué/qué/cómo/qué cambia hoy”). Mensaje central uniforme, breve y verificable, que conecte la mejora de integridad y trazabilidad con beneficios para usuarios y auditores (Kotter, 2012).

Canales y cadencia. Lanzamiento (townhall), boletines quincenales, FAQ vivas, micrositio interno, cartelera digital, y oficinas abiertas semanales con el equipo del piloto; repositorio de decisiones y changelog funcional (NIST, 2018).

Gestión de consultas e incidencias. Mesa funcional (nivel 1) con acuerdos de servicio y escalamiento a nivel técnico/seguridad/legal (ISO/IEC 27001:2022).

Acompañamiento en el puesto. Shadowing en las dos primeras semanas de operación y coaching a “usuarios clave”, con registro de dudas frecuentes para retroalimentar materiales (Hiatt, 2006).

6.7.3 Formación por perfil (currícula, evaluación y certificación)

Estructura general. Módulos modulares y cortos (microlearning) + prácticas guiadas en laboratorio/sandbox + evaluación y certificación por rol. Todas las sesiones incluyen objetivos, prerequisites, checklist de competencias, y criterios de aprobación $\geq 80\%$. a) Usuarios de gestión (2–3 h). Operación diaria, carga/validación de hitos, consultas en el tablero, contingencias y flujos de corrección excepcional; práctica con casos anonimizados. b) Auditores internos/externos (3–4 h). Lectura de manifiestos, verificación de hash/txid y pruebas de inclusión Merkle, recreación de rastro y papeles de trabajo reproducibles; criterios de evidencia suficiente y apropiada (INTOSAI, 2013). c) Técnicos (4–6 h).

Contratos inteligentes (ciclo de vida y controles), anclaje multired, gestión de llaves/seguridad, ETL y reconciliaciones on/off-chain; runbooks y observabilidad (NIST, 2018; ISO/IEC 27001:2022). d) Legales/Datos (2–3 h). Validez probatoria (firma/sello), publicación responsable (transparencia con test de daño) y protección de datos (minimización, seudo/anonimización, retención) con ejercicios de clasificación de datos (Ley 25.326, 2000; Ley 27.275, 2016). Evaluación. Cuestionario teórico + prueba práctica (checklist por rol). Recertificación anual o ante cambios materiales del sistema (ISO, 2018).

6.7.4 Prácticas y simulacros

Laboratorio de auditoría (mensual). Casos reales anonimizados: verificación de huellas, recreación de rastro, detección de divergencias on/off-chain y documentación de hallazgos (INTOSAI, 2013).

Simulacros de incidentes (trimestral). Tabletop y ejercicios cronometrados para respuesta a incidentes, revocación/rotación de llaves y reintentos de anclaje, midiendo RTO/RPO efectivos (NIST, 2018; ISO, 2018).

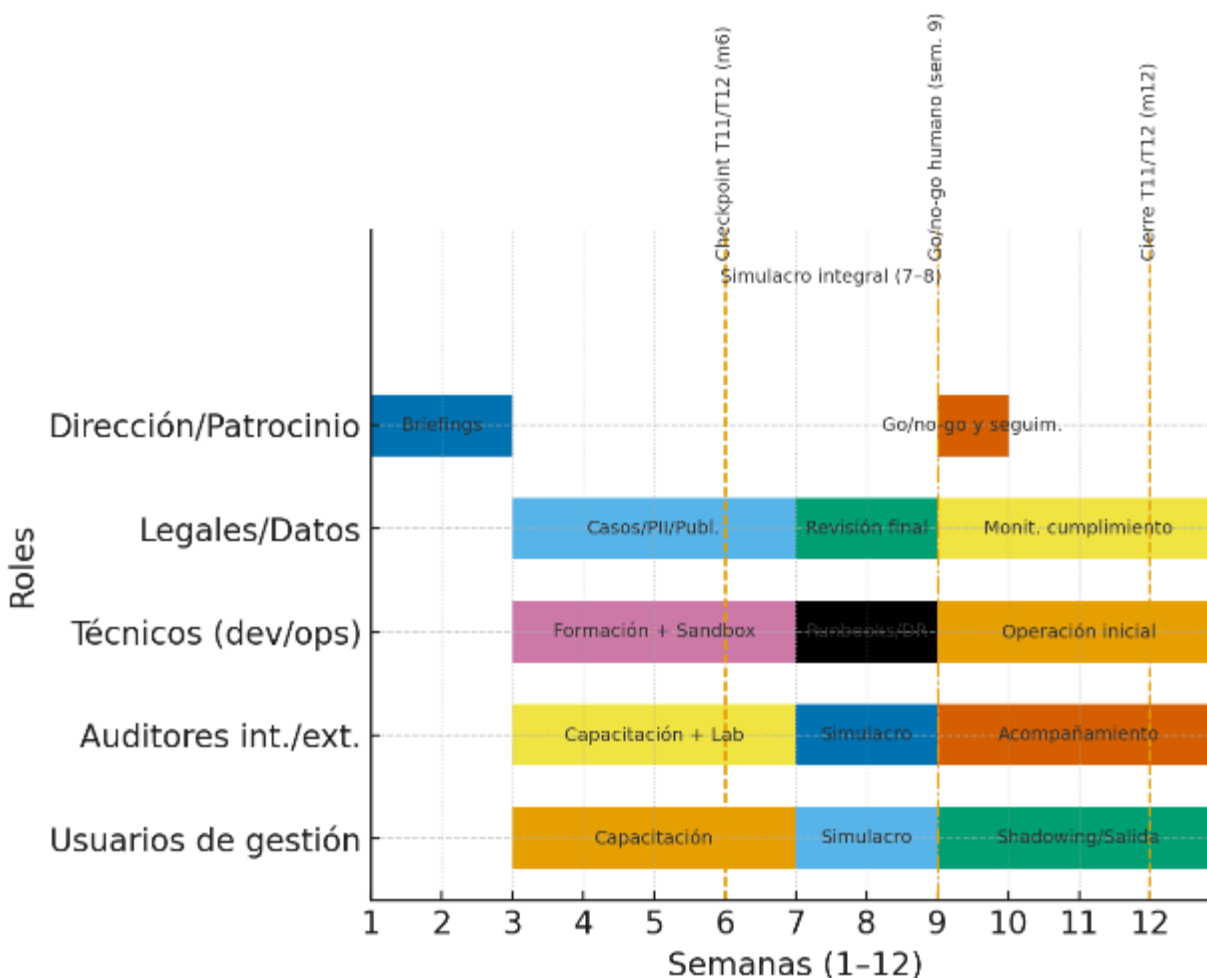
Práctica de continuidad. Restauración desde backup, integración con SIEM, y validación de sellos de tiempo y trazabilidad post-evento (ISO/IEC 27001:2022).

La Figura 69 sintetiza el cronograma de adopción y capacitación para las primeras 12 semanas, articulando actividades, hitos y métricas de avance. La secuencia incorpora un hito go/no-go humano en la semana 9, condicionado por los niveles de dominio y confianza reportados por los distintos roles.

6.7.5 Cronograma, responsabilidades, métricas y refuerzo

Figura 69

Cronograma de adopción y capacitación (12 semanas) con métricas de avance.



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en el plan de capacitación y de las métricas de adopción (T11, T12) y del hito operativo go/no-go humano en la semana 9. Abreviaturas: PII = información personal identificable; DR Drill = simulacro de recuperación ante desastres.

Cronograma (12 semanas). Semanas 1–2: Lanzamiento, línea base de adopción, pilotos de materiales. Semanas 3–6: Capacitación por rol + laboratorio/sandbox. Semanas 7–8: Simulacro integral y ajustes. Semanas 9–12: Salida gradual y shadowing en producción.

Responsables. Cambio/Capacitación (diseño e impartición), Dirección OA (patrocinio y decisiones), Auditoría (laboratorio y aseguramiento), Legal/Datos (publicación responsable), Seguridad/DevOps (simulacros).

Métricas (vinculadas a 6.6). T11 satisfacción ($\geq 4,2/5$ con IC95 %), T12 personal crítico certificado (≥ 90 % mes 3; 100 % mes 6); asistencia ≥ 80 %, intentos de examen ≤ 2 por persona, cierre de brechas ≤ 30 días (INTOSAI, 2013; ISO, 2018).

Refuerzo. Red de champions por área, booster sessions bimensuales de 45', tips semanales (“1 cosa que cambió”), y reconocimiento a buenas prácticas (Hiatt, 2006; Kotter, 2012).

Criterio de aceptación del cambio (go/no-go humano). ≥ 95 % de usuarios críticos habilitados (capacitados + aprobados), caída ≥ 30 % de tickets de “uso” tras 30 días y cero incidentes críticos atribuibles a desconocimiento (INTOSAI, 2013; NIST, 2018).

Materiales y soportes. Manuales por rol, videos cortos (≤ 6 min), guías de verificación ciudadana, FAQ vivas, checklists de evidencias y runbooks; todos versionados y con fecha de vigencia. Cada material explicita objetivo, alcance, responsables y base legal aplicable (ISO, 2018; ISO/IEC 27001:2022).

La Tabla 63 detalla el cronograma de capacitación por rol, vinculando cada actividad con métricas de adopción y confianza. De este modo, la evaluación del entrenamiento no se limita a la asistencia, sino que incorpora indicadores de comprensión, práctica guiada y preparación para operar en producción.

Tabla 63*Cronograma de capacitación por rol y métricas de adopción (Capacitación)*

Rol	Contenidos	Horas	Eval.	Métrica	Resp.
Usuarios gestión	Operación; carga/valid.; consultas; conting.	2–3 h + microlearning	Teórico+práct .; ≥80%	T12; asis. ≥80%	Cambio/Cap.
Audidores int./ext.	Manifiestos; hash/txid; Merkle; rastros	3–4 h + lab mensual	Teórico+práct .; ≥80%	T11; T12	Auditoría
Técnicos (dev/ops)	Contratos; anclaje; llaves; ETL; runbooks/obs.	4–6 h + sandbox	Teórico+práct .; ≥80%	T8; T10; T12	Seg/SRE
Legales/Datos	Validez probatoria; publ. responsable; PII	2–3 h + casos	Teórico+práct .; ≥80%	T7; T12	Legal/Datos
Dirección/Patroc.	Objetivos; riesgos; métricas; go/no-go	1–2 h (briefing)	Chequeo de comprensión	T11	Dir OA

Nota. Elaboración propia. Abreviaturas: IC95% = intervalo de confianza del 95 %; go/no-go = hito de decisión operacional; shadowing = acompañamiento en producción. Las métricas de adopción se vinculan con T11–T12 y con la continuidad de T10 (ISO 19011, 2018; INTOSAI, 2013).

Complementariamente, la Tabla 64 organiza el mismo plan de capacitación en clave temporal (por semanas), resaltando la concentración de actividades por rol y los momentos de mayor carga. Esta vista facilita la coordinación logística y la asignación de tiempo a tareas de formación sin comprometer la operación regular.

Tabla 64*Cronograma de capacitación por rol y métricas de adopción (Semanas)*

Semana	Hitos
1–2	Lanzamiento; línea base; pilotos
3–6	Capacitación por rol + laboratorio/sandbox
7–8	Simulacro integral y ajustes
9–12	Salida gradual y shadowing

Nota. Elaboración propia. Abreviaturas: IC95% = intervalo de confianza del 95 %; go/no-go = hito de decisión operacional; shadowing = acompañamiento en producción. Las métricas de adopción se vinculan con T11–T12 y con la continuidad de T10 (ISO 19011, 2018; INTOSAI, 2013).

6.8 Riesgos y mitigación

Esta sección consolida el registro de riesgos del piloto, los controles preventivos y detectivos, los planes de contingencia y los umbrales de escalamiento. La gestión se alinea con criterios de evidencia suficiente y apropiada y con marcos de control interno y auditoría (INTOSAI, 2013), seguridad de la información (ISO/IEC 27001:2022; NIST, 2018) y lineamientos técnico-operativos del diseño híbrido (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020). Se adoptan estrategias evitar / reducir / transferir / aceptar y se monitorea con los indicadores de 6.6 (T1–T12).

6.8.1 Taxonomía y apetito de riesgo

Técnicos: consenso, llaves, disponibilidad, rendimiento, integridad de evidencias.

Legales y de datos: validez probatoria, privacidad, transparencia responsable.

Organizacionales y de adopción: roles, SoD, capacitación, cambio cultural.

Continuidad y terceros: dependencia de proveedores, obsolescencia, DR/BCP.

Reputacionales y de comunicación: percepción pública, trazabilidad publicada.

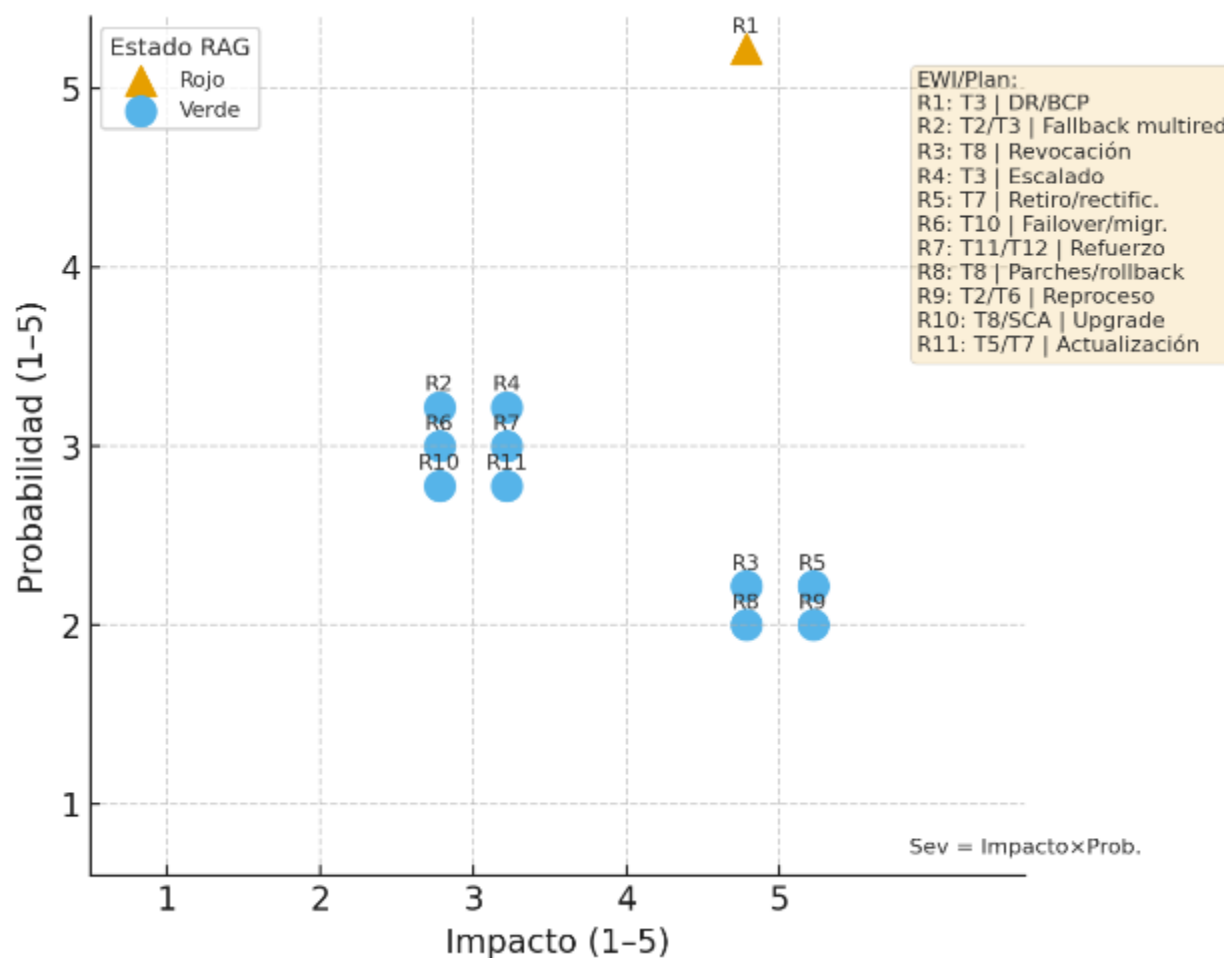
Apetito de riesgo: cero tolerancia a incidentes de integridad/validez probatoria y a exposición de datos personales; tolerancia baja a indisponibilidad (SLA), media a latencias de anclaje si no afectan verificabilidad, y media a reintentos por comisiones si se cumple el “fee cap” (NIST, 2018; ISO/IEC 27001:2022).

6.8.2 Registro de riesgos y mitigación (resumen operativo)

La Figura 70 muestra el mapa de riesgos del piloto en un esquema de heatmap probabilidad×impacto. Cada marcador representa un riesgo identificado, su severidad relativa y su estado RAG, permitiendo visualizar de un vistazo los focos que requieren mitigaciones prioritarias o una revisión del diseño.

Figura 70

Mapa de riesgos del piloto (heatmap probabilidad×impacto)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. El tamaño del marcador representa la severidad (impacto × probabilidad). El estado RAG se codifica por forma del marcador (▲ = Rojo, ■ = Ámbar, ● = Verde) con la siguiente regla: Rojo (≥ 20), Ámbar (12–19) y Verde (≤ 11). Para evitar solapes, los riesgos que comparten celda se muestran en subposiciones discretas y se incluye una caja lateral con el mapeo $R\# \rightarrow \text{EWI} \mid \text{Plan}$. Mapeo cualitativo utilizado: Probabilidad (Baja = 2; Media = 3; Alta = 5) e Impacto (Bajo = 2; Medio = 3; Alto = 5). Abreviaturas: EWI = Early Warning Indicator; RAG = Rojo/Ámbar/Verde; DR/BCP =

Recuperación/Continuidad; ETL = Extracción, Transformación y Carga; CVE = Vulnerabilidad Común; SCA = Software Composition Analysis.

R1. Colusión o fallas de validadores.

Causa raíz: número insuficiente de validadores, configuración laxa, llaves sin rotación.

Impacto: pérdida de liveness/consenso, riesgo de indisponibilidad o manipulación.

Prevención: consenso QBFT/PBFT (3–5 validadores), segregación de nodos, hardening y auditorías de configuración; rotación de llaves y custodia con KMS/HSM; SoD en operación.

Detección: T3 (SLA); health checks de consenso; alertas de desalineación temporal.

Contingencia: failover de validador, reseed desde snapshots firmados, DR/BCP.

Dueño: Arquitectura/SRE. (ISO/IEC 27001:2022; NIST, 2018)

R2. Congestión o tarifas altas en cadenas públicas.

Causa raíz: picos de uso/redes públicas; gas price alto.

Impacto: retraso en anclajes, aumento de costos.

Prevención: política multired con ventanas de consolidación y batching; fee cap y colas de reintento; fallback a red secundaria.

Detección: T2 (verificación de anclaje), T3 (latencia doc→anclaje), métricas de costo por lote.

Contingencia: posponer a ventana de menor congestión; activar tercera red mensual; “grace period” documentado en manifiesto.

Dueño: SRE/Datos. (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; NIST, 2018)

R3. Pérdida/compromiso de claves (operativas o de servicio).

Causa raíz: almacenamiento inseguro, ausencia de MFA/doble intervención, prácticas débiles.

Impacto: firmas inválidas, acceso no autorizado, ruptura de cadena de custodia.

Prevención: KMS/HSM, MFA, política 4 ojos para operaciones críticas, rotación trimestral, just-in-time access, bóveda fuera de línea para copias selladas.

Detección: alertas SIEM por uso anómalo; auditorías de acceso; T8.

Contingencia: revocación y re-emisión de certificados; key ceremony; re-sello de manifiestos si corresponde.

Dueño: Seguridad/Legal. (ISO/IEC 27001:2022; INTOSAI, 2013)

R4. Rendimiento/latencia en registro y ETL.

Causa raíz: picos de carga, colas subdimensionadas, contratos ineficientes.

Impacto: demoras de anclaje, caída de T3.

Prevención: pruebas de carga, colas asíncronas con backpressure, optimización de contratos, circuit breakers.

Detección: T3 (P95 de latencia), dashboards de colas, reintentos.

Contingencia: escalar horizontal, ampliar ventana de batching sin perder verificabilidad.

Dueño: Integración/SRE. (NIST, 2018)

R5. Exposición de datos personales o sensibles.

Causa raíz: mapeo deficiente de metadatos, publicación sin anonimización, errores de perfilamiento de acceso.

Impacto: incumplimiento legal, daño reputacional.

Prevención: minimización y seudonimización/anonimización; on/off-chain por diseño; EIPD/DPIA en tratamientos de riesgo; control de acceso por necesidad de saber; revisión legal previa.

Detección: T7 (calidad de metadatos), revisiones de Legal/Datos, auditorías de catálogo.

Contingencia: takedown inmediato, hotfix de visibilidad, notificación según normativa.

Dueño: Legal/Datos. (Ley 25.326, 2000; ISO/IEC 27001:2022)

R6. Impugnación de validez probatoria.

Causa raíz: firmas fuera de IFD, sellos inválidos, metadatos incompletos, relojes desincronizados.

Impacto: cuestionamiento de evidencias y manifiestos.

Prevención: firma digital conforme Ley 25.506, sellado de tiempo confiable, sincronización NTP/PTP redundante, manifiesto con raíz Merkle + txid + altura + algoritmo; double-check de cadena de confianza.

Detección: T2; validaciones criptográficas programadas; linting de manifiestos.

Contingencia: re-sello y re-anclaje con referencia cruzada; dictamen legal respaldatorio.

Dueño: Legal/Arquitectura. (Ley 25.506, 2001; INTOSAI, 2013)

R7. Resistencia al cambio y desplazamiento de prácticas.

Causa raíz: incertidumbre, fricción de uso, falta de beneficios visibles.

Impacto: baja adopción, errores de operación, workarounds.

Prevención: plan de gestión del cambio (6.7), quick wins, red de champions, formación por rol y shadowing.

Detección: T11 (satisfacción), T12 (certificación), tickets de uso por 1.000 transacciones.

Contingencia: refuerzo focalizado, ajustes de UX y procesos, incentivos.

Dueño: Cambio/Capacitación. (INTOSAI, 2013; ISO, 2018)

R8. Desalineación de responsabilidades y SoD.

Causa raíz: RACI ambiguo, acumulación de privilegios, urgencias operativas.

Impacto: riesgos de fraude o errores no detectados.

Prevención: RACI explícito, segregación de funciones (SoD), access reviews mensuales.

Detección: T9 (conformidad COSO/ISSAI), revisiones de acceso y joiner-mover-leaver.

Contingencia:access freeze, re-asignación de roles, auditoría puntual.

Dueño: Dirección OA/Seguridad. (COSO, 2013; INTOSAI, 2013)

R9. Dependencia de terceros / proveedores.

Causa raíz: servicios gestionados críticos (KMS, SIEM, nube).

Impacto: indisponibilidad, vendor lock-in, barreras de salida.

Prevención:cláusulas de salida, reversibilidad y escrow; uso de estándares abiertos, documentación completa y infra como código.

Detección: T10 (continuidad), auditorías de nivel de servicio.

Contingencia:failover a secundario, runbook de migración, pruebas de reversibilidad.

Dueño: Dirección/Compras/SRE. (ISO/IEC 27001:2022; NIST, 2018)

R10. Obsolescencia tecnológica.

Causa raíz: cambios en protocolos/redes, bibliotecas vulnerables, deprecaciones.

Impacto: incompatibilidades, brechas de seguridad.

Prevención:vigilancia tecnológica, dependabot/SBOM, ciclo de actualizaciones planificadas y pruebas en staging.

Detección: T8, reportes de CVE, escaneo SCA/DAST.

Contingencia:upgrade path documentado, roll-back, parches de seguridad.

Dueño: Arquitectura/DevOps. (NIST, 2018; ISO/IEC 27001:2022)

R11. Riesgo reputacional por publicación incompleta o tardía.

Causa raíz: demoras en curaduría de datasets, metadatos deficientes, conflictos transparencia-privacidad.

Impacto: pérdida de confianza pública.

Prevención:matriz de publicación selectiva (6.5), SLA de publicación, revisión Legal/Datos, data steward por dataset.

Detección: T7 (cobertura de publicación), T5 (rastros completos), consultas y quejas.

Contingencia: actualización prioritaria, aclaración pública y release notes; plan de comunicación.

Dueño: Transparencia/Legal. (Ley 27.275, 2016; Ley 25.326, 2000)

La Tabla 65 desarrolla el registro de riesgos del piloto, especificando descripción, dueño, mitigaciones previstas e indicadores tempranos (EWI), junto con su estado RAG. Este registro opera como complemento textual del heatmap y como insumo operativo para el seguimiento periódico de riesgos.

Tabla 65*Registro de riesgos del piloto, mitigaciones y EWI/RAG*

Riesgo	Causa	P/I	Owner	Mitig.	EWI	RAG	Conting.
R1 Colusión/falla valid.	Validadores insuf.; config. laxa; llaves sin rot.	Alta/Alto	Arq/SRE	QBFT/PBFT; hardening; KMS/HSM; rotación	T3; health-checks	Rojo: P95>36h ×2	Failover; reseed; DR/BCP
R2 Congestión/fees públicos	Picos de gas	Media/Medio	SRE/Datos	Fee-cap; ventanas; batching; fallback multired	T2; T3; costo/lot	Ámbar: reint.>10%	Posponer; 3ª red; grace
R3 Pérdida/compromiso de claves	Prácticas débiles; sin MFA	Baja/Alto	Seg/Legal	KMS/HSM; 4-ojos; rotación; JIT	T8; SIEM	Rojo: incidente crítico	Revoc.; re-emisión; key ceremony
R4 Rendimiento/latencia	Picos; colas subdim.; contratos inef.	Media/Medio	Int/SRE	Pruebas carga; backpressure; optimización	T3; dashboards	Ámbar: cerca umbral	Escalado; ampliar ventana
R5 Exposición de datos	Publicación sin anonimización	Baja/Alto	Legal/Datos	Minimización; pseudo/anon.; acceso	T7; quejas	Rojo: hallazgo severo	Retiro/rectificación
R6 Dependencia de terceros	Proveedor único; lock-in	Media/Medio	Dir/Compras/SRE	SLA; multicloud; IaC	T10; aud. SLA	Ámbar: degradación	Failover; migración
R7 Adopción/uso insuf.	Resistencia; baja capacitación	Media/Medio	Cambio/Cap.	Comunicación; formación; shadowing	T11; T12; tickets	Ámbar: tickets ↑20%	Refuerzo/coaching
R8 Incidentes de seguridad	Vulns.; malas prácticas	Baja/Alto	Seg/SRE	SAST/DAST; hardening; revisión	T8; CVE	Rojo: crítico	Parches; rollback; RCA
R9 Integridad de evidencias	Errores ETL/firmas	Baja/Alto	Datos/SRE	Runbooks; reconc.; pruebas Merkle	T2; T6	Ámbar: T6>1%	Reproceso; corrección
R10 Obsolescencia tecn.	Cambios protocolo/libros	Media/Medio	Arq/SRE	SBOM; actualizaciones	T8; SCA/DAST	Ámbar: CVE altas	Upgrade; rollback
R11 Riesgo reputacional	Publicación tardía/incompleta	Media/Medio	Transp/Legal	SLA publicación; revisión legal	T5; T7	Ámbar: T5<85%	Act. prioritaria; comunicación

Nota. Elaboración propia. Abreviaturas: EWI = Early Warning Indicator; RAG = Rojo/Ámbar/Verde; BCP/DR = continuidad/recuperación; QBFT/PBFT = algoritmos tolerantes a fallas bizantinas. Los umbrales se alinean con T2, T3, T6, T8 y T10–T12 (INTOSAI, 2013; NIST, 2018; ISO, 2018).

A los riesgos técnicos y operativos identificados corresponde añadir ciertos riesgos de naturaleza tecno-institucional. En primer lugar, la dependencia de proveedores tecnológicos críticos —en particular, servicios de nube, custodia criptográfica, monitoreo, soporte especializado o integraciones específicas— podría generar escenarios de lock-in, dificultar la portabilidad de la solución, encarecer su continuidad o condicionar decisiones futuras de arquitectura. Como medidas de mitigación, se propone priorizar componentes basados en estándares abiertos, separar la lógica de negocio de la infraestructura subyacente, documentar interfaces e integraciones críticas y prever, desde etapas tempranas, criterios de portabilidad y estrategia de salida de proveedor.

En segundo lugar, la continuidad del piloto podría verse afectada por cambios de gestión, redefiniciones de prioridades político-administrativas o reasignaciones presupuestarias, aun cuando los resultados técnicos iniciales fueran satisfactorios. Para mitigar este riesgo, resulta conveniente formalizar el patrocinio institucional, alinear el piloto con objetivos de control, transparencia y eficiencia ya reconocidos por la organización, y estructurar una implementación por etapas con entregables verificables que faciliten su sostenimiento frente a eventuales cambios de conducción.

En tercer lugar, la sostenibilidad organizacional del proyecto depende de que el conocimiento técnico y operativo no quede concentrado en pocos actores o contratistas, dado que ello reduciría la autonomía institucional del organismo para sostener, auditar o escalar la solución. A tal efecto, se recomienda asegurar transferencia efectiva de capacidades al personal interno, mantener documentación funcional y técnica actualizada, definir procedimientos operativos claros y distribuir responsabilidades críticas entre distintos perfiles del organismo, a fin de reducir puntos únicos de dependencia.

6.8.3 Señales tempranas (EWI) y umbrales de escalamiento (RAG)

Rojo (escalamiento inmediato a Comité): T2 < 95 % en el mes; T3 P95 > 36 h en dos cortes; incidente T8 crítico; hallazgo legal severo.

Ámbar (plan de acción en 5 días): T5 < 85 %; T6 > 1 %; reintentos de anclaje > 10 % del total; tickets de uso ↑ 20 % dos meses seguidos.

Verde (operación normal): metas de 6.6 cumplidas o tendencia favorable ≥ 2 meses.

6.8.4 Plan de anclaje híbrido (operación y contingencias)

La Tabla 66 resume la política de anclaje multired, incluyendo redes de destino, frecuencias, parámetros operativos y respuestas ante contingencias. El objetivo es garantizar prueba de existencia e integridad aun cuando se degraden las condiciones de la red primaria o se activen límites de costo (fee cap).

Tabla 66

Política de anclaje multired y contingencias

Red	Cad.	Ventana/batch	Fee-cap	Fallback	Manifiestos	Resp.
Primaria (Ethereum)	Diaria	Ventana 24 h; raíz Merkle por lote	Fee-cap gob.	Secundaria	Manifiesto firmado (txid, altura, raíz, algoritmo, ventana)	SRE
Secundaria (Bitcoin)	Semanal	Batch fuera de picos	Fee-cap semanal	Terciaria	Manifiesto firmado + conf. mín.	SRE
Terciaria (respaldo)	Mensual	Batch mensual	Fee-cap mensual	Dif. documentado	Manifiesto aun si se difiere	SRE + Auditoría

Nota. Elaboración propia. Abreviaturas: txid = identificador de transacción; raíz de Merkle = hash que resume el conjunto de evidencias del lote; fee-cap = tope de comisión; fallback = red alternativa. Cada lote documenta un manifiesto firmado (txid, altura de bloque, raíz, algoritmo, ventana) (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; NIST, 2018; ISO/IEC, 2022).

El esquema prevé anclaje diario en la red primaria (por ejemplo, Ethereum) con una raíz de Merkle por lote y manifiesto firmado; anclaje semanal en una red secundaria (por ejemplo, Bitcoin) y anclaje mensual en una tercera red de respaldo.

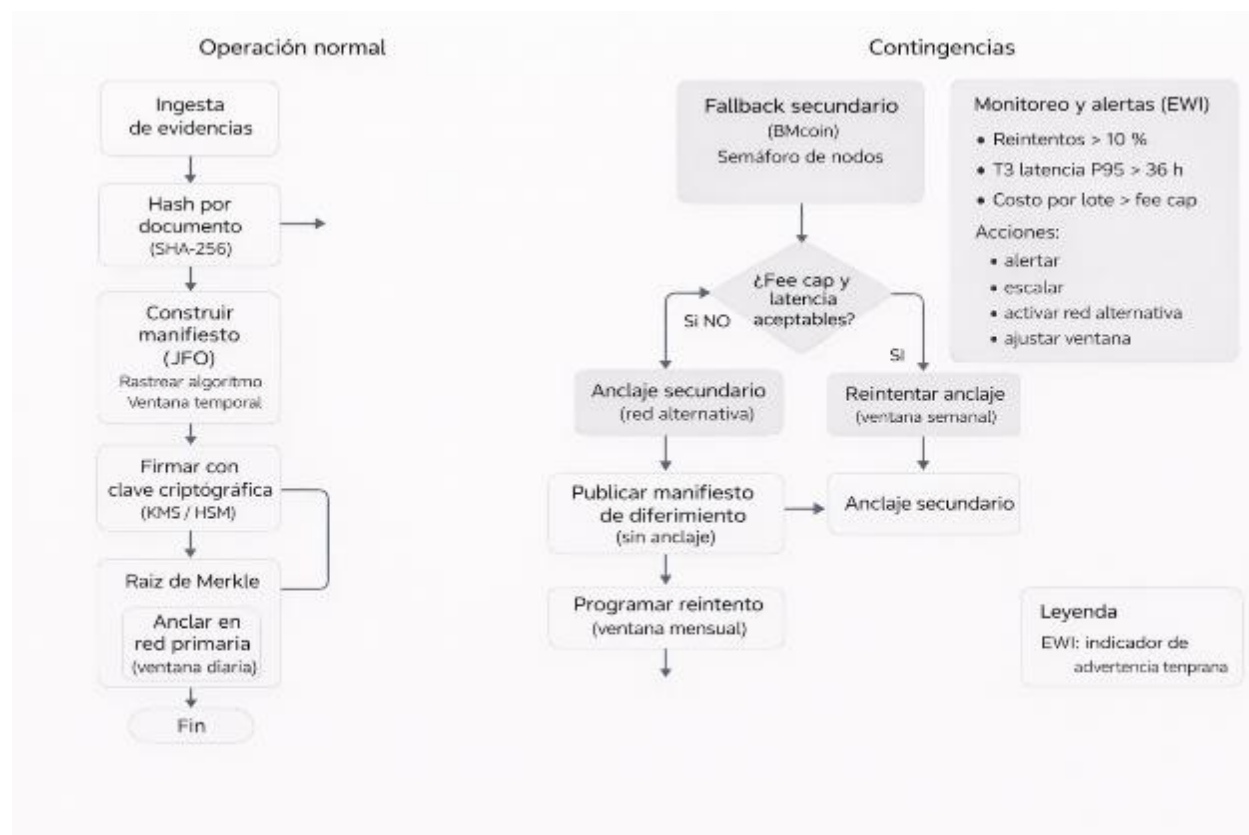
Las contingencias se gestionan mediante: multired, selección de ventanas según el nivel de comisiones, reintentos automáticos y confirmaciones mínimas. Si una ventana no se puede anclar, el sistema publica igualmente el manifiesto de diferimiento, documenta la causa y programa un nuevo intento dentro de la ventana siguiente (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La Figura 71 representa la política de anclaje híbrido en operación normal (ingesta de evidencias, cálculo de hashes por documento, raíz de Merkle, manifiesto firmado y anclaje primario diario) y en escenarios de contingencia (monitoreo de indicadores tempranos, verificación de fee cap y latencia, activación de red secundaria o terciaria, y generación de manifiestos de diferimiento cuando corresponda). Cada manifiesto incluye txid, altura de bloque, raíz de Merkle, algoritmo de hash y ventana de consolidación, y se firma con claves institucionales gestionadas en KMS/HSM bajo esquema de cuatro

ojos. Los umbrales de disparo se alinean con T2–T3 (por ejemplo, reintentos > 10 %, P95 > 36 h, costo por lote superior al fee cap). Marcos de referencia: NIST (2018); ISO/IEC 27001:2022; INTOSAI (2013); Foro Económico Mundial & Banco Interamericano de Desarrollo (2020); AAIP (2018).

Figura 71

Política de anclaje híbrido multired (operación y contingencias)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor con base en NIST, 2018; ISO/IEC 27001:2022; INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; AAIP, 2018.

6.8.5 Gobernanza del riesgo y verificación independiente

Comité de Gobernanza revisa el registro de riesgos mensualmente y al cierre de hitos; ajusta umbrales, aprueba cambios mayores y ordena auditorías ad-hoc.

Aseguramiento independiente (Auditoría interna): prueba la suficiencia y apropiación de evidencias, replica verificaciones de hash/txid y cotejos on/off-chain, y emite management letter con acciones y plazos (INTOSAI, 2013; ISO 19011:2018).

6.9 Resumen

El plan piloto propuesto articula una arquitectura híbrida —red permitida para la operación cotidiana y anclaje periódico en cadena pública— con reglas claras de firma digital, sellado de tiempo y publicación selectiva, de modo que la evidencia técnica (hashes, raíces de Merkle, txid, sellos) se transforme en evidencia suficiente y apropiada bajo estándares de control. El alcance acotado (ejecución presupuestaria y contrataciones de la OA) permite impacto temprano y aprendizaje controlado, mientras que el diseño modular (identidad y llaves, registro de evidencias, ETL de metadatos, tablero de verificación) sienta bases para escalabilidad y replicabilidad en otras áreas del Estado. La gobernanza —con comité mixto, segregación de funciones y aseguramiento independiente— asegura trazabilidad de decisiones, administración de riesgos y revisión por terceros. En paralelo, la privacidad por diseño y el control on/off-chain sostienen el equilibrio entre validez probatoria, integridad y protección de datos, sin sacrificar transparencia ni verificabilidad externa (COSO, 2013; INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

La medición se apoya en un set compacto y reproducible de indicadores T1–T12 que cubren eficiencia y control (tiempos de auditoría, latencia documento→anclaje, disminución de observaciones), transparencia y trazabilidad (rastreo licitatorio completo, divergencias on/off-chain, cobertura de publicación activa), seguridad y continuidad (incidentes, conformidad con marcos de control, RTO/RPO efectivo) y adopción (satisfacción y certificación por rol). Estos indicadores cuentan con línea de base prepiloto, umbrales RAG y metas de corto/mediano plazo, habilitando correcciones con evidencia y decisiones go/no-go. El plan de gestión del cambio agrega comunicación de propósito público, formación por perfil y prácticas con casos reales, reduciendo fricción operativa e incrementando la confianza en la evidencia.

Desde la perspectiva de control público, el valor emerge cuando cada hito del proceso genera pruebas verificables por terceros mediante procedimientos reproducibles: huellas recalculables, manifiestos firmados y verificaciones de inclusión que se alinean con criterios de suficiencia y apropiación de la evidencia y con actividades de control bien definidas. En términos técnico-económicos, la estrategia de anclaje por lotes y política multired mantiene costos predecibles y resiliencia frente a congestión, mientras que la reutilización de infraestructura estatal (PKI/TSA, observabilidad, archivo electrónico) reduce CAPEX/OPEX. En suma, el piloto equilibra integridad técnica, validez probatoria y protección de datos, provee métricas objetivas y gobernanza efectiva y maximiza la transferibilidad del modelo a otras instituciones con mínimos ajustes (COSO, 2013; INTOSAI, 2013; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Capítulo 7: Evaluación e impacto

7.1 Comparación con modelos tradicionales

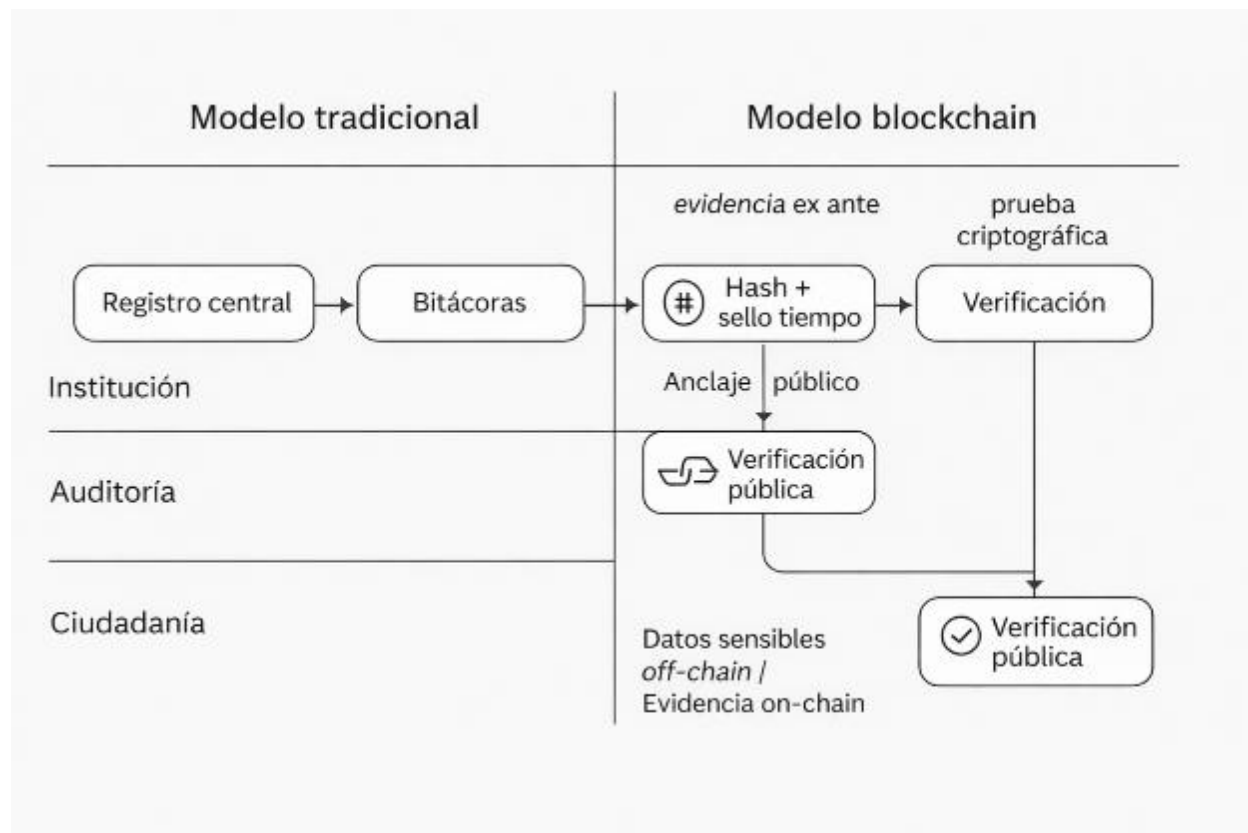
En los modelos tradicionales de gestión y contabilidad pública —basados en sistemas centralizados (por ejemplo, SIGAF/ERP), registros de doble entrada y controles ex post— la integridad de la información se respalda en procedimientos administrativos y auditorías documentales. La propuesta basada en blockchain desplaza parte de este aseguramiento hacia el propio diseño del sistema: un libro mayor distribuido, con consenso criptográfico e inmutabilidad que actúa como “control interno tecnológico” ex ante y complementa, sin sustituir, los mecanismos de control interno y externo existentes.

Desde una perspectiva epistemológica, el cambio es de medio y de método. Los sistemas tradicionales confían principalmente en la autoridad institucional y en la evidencia documental centralizada; blockchain confía en reglas formales verificables por múltiples pares, donde la prueba de integridad es matemática y reproducible. En términos generales, la ciencia aplicada a la gestión pública requiere un “conocimiento racional, sistemático, exacto, verificable y por consiguiente falible”, de modo que toda innovación tecnológica debe poder someterse a contrastación y auditoría (Bunge, 2004, p. 6). En este sentido, blockchain aporta una capa adicional de verificabilidad técnica y nuevas trazas auditables.

En el marco de este trabajo, blockchain se define operativamente como un “libro contable inmutable y abierto” orientado a fortalecer transparencia y trazabilidad en el Estado (p. 2). Esta definición fija la base de comparación con los modelos previos, en los que la inmutabilidad depende de políticas de resguardo y gobernanza sobre bases de datos editables y más expuestas a errores o manipulaciones no detectadas a tiempo. La Figura 72 contrasta el flujo de evidencia en un esquema tradicional, apoyado en documentos y bitácoras ex post, con un modelo basado en blockchain que incorpora evidencias criptográficas y anclaje público desde el inicio del ciclo. El contraste permite observar cómo cambia el momento en que se generan las garantías de integridad y trazabilidad y qué implicancias tiene esto para la auditoría y el control ciudadano.

Figura 72

Flujo de evidencia: modelo tradicional vs. blockchain



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. El diagrama contrasta controles ex post basados en documentos y bitácoras con garantías ex ante sustentadas en evidencias criptográficas (hash y sello de tiempo) y anclaje público, habilitando verificación por terceros (auditoría/ciudadanía). Los datos sensibles permanecen off-chain bajo control institucional; sólo se publican evidencias on-chain (compromisos/huellas). Abreviaturas: on-chain = en cadena; off-chain = fuera de cadena; hash = resumen criptográfico; TSP = protocolo de sellado de tiempo.

Esta arquitectura híbrida —que combina dominio institucional y prueba pública de integridad— no tiene un equivalente funcional directo en los modelos tradicionales. En éstos, la validación de integridad se prueba mediante cadena de custodia documental y controles de acceso; en blockchain, se fundamenta en anclajes criptográficos y consenso distribuido. En complemento con la Figura 72, la Tabla 67 resume las diferencias clave entre los modelos tradicionales de registro contable y la propuesta basada en blockchain, organizando la comparación por dimensiones de control, trazabilidad y auditoría e indicando qué aspectos se mantienen, cuáles se refuerzan y qué capacidades nuevas se incorporan.

Tabla 67*Comparación sintética entre modelos tradicionales y la propuesta basada en blockchain*

Dimensión	Modelos tradicionales (doble entrada + ERP/SIGAF)	Propuesta con blockchain (libro mayor distribuido)
Integridad de datos	Garantizada por controles internos, bitácoras de BD y auditoría ex post	Inmutabilidad por diseño; pruebas criptográficas y consenso; evidencias ex ante
Trazabilidad	Logs de aplicación y documentos; reconstrucción costosa	Trazas encadenadas por bloque/tx; reconstrucción nativa y verificable
Evidencia y cadena de custodia	Documental, dependiente de repositorios y firmas	Evidencia hash-time (anclajes) y sellos de tiempo distribuidos
Acceso y publicidad	Predominio de acceso interno; publicación selectiva	Separación dato/compromiso: capas privadas + anclajes públicos verificables
Riesgo de manipulación	Riesgo humano/técnico mitigado por controles	Altamente disuasivo por inmutabilidad y detectabilidad de cambios
Auditoría	Muestras y pruebas sustantivas/ de cumplimiento	“Reejecución” y verificación criptográfica; reducción de pruebas repetitivas
Interoperabilidad	Integraciones por ETL/servicios; esquemas heterogéneos	Estándares de eventos/formatos; anclajes comunes, identidades verificables
Costos de verificación	Elevados en procesos complejos y multi-actor	Disminuyen al externalizar verificación a la red (verificabilidad por terceros)
Gobernanza	Jerárquica, basada en roles y perfiles	Multiactor: reglas codificadas + política de nodos/consorcio
Privacidad	Controlada por el sistema central	Criptografía aplicada (hashing, ZKPs, permisos) + política de revelación

Nota. Elaboración propia. Comparación conceptual basada en atributos de control, trazabilidad y auditoría entre modelos tradicionales (ERP/SIGAF) y un libro mayor distribuido con anclaje público. La matriz no implica sustitución de controles legales ni de auditoría; la propuesta complementa el control interno y externo con verificabilidad criptográfica ex ante. Abreviaturas: ERP = planificación de recursos empresariales; SIGAF = Sistema Integrado de Gestión y Administración Financiera; BD = base de datos;

ETL = extracción, transformación y carga; API = interfaz de programación de aplicaciones; Tx = transacción; ZKP = prueba de conocimiento cero.

La contabilidad de doble entrada, pilar de los modelos tradicionales, asegura equilibrio lógico pero no garantiza por sí misma la inmutabilidad del registro. La contabilidad de “triple entrada” asociada a blockchain añade un tercer comprobante criptográfico y compartido que se convierte en evidencia objetiva de cada asiento: un recibo firmado y encadenado que cualquier parte autorizada puede verificar sin alterar. En la práctica, esto desplaza parte del problema de “confianza institucional” hacia un problema de “verificación técnica”, reduciendo asimetrías de información y tiempos de conciliación.

En los modelos tradicionales, el aseguramiento depende de la calidad del control interno y del muestreo de auditoría; en blockchain, una porción del aseguramiento se estandariza en el protocolo. Esta diferencia metodológica sugiere cambios en el enfoque de auditoría: se pasa de probar transacciones individuales a validar reglas, estados y evidencias criptográficas, en línea con un paradigma de investigación aplicada sistemática, controlada, empírica y crítica.

Frente a un modelo centrado en confianza, documentos y controles internos, blockchain introduce un modelo centrado en verificabilidad, evidencias criptográficas y gobernanza compartida, más coherente con los principios de trazabilidad y rendición de cuentas que demanda la gestión pública contemporánea.

7.2 Beneficios esperados

La implementación de una arquitectura híbrida de blockchain en la gestión pública —con registro distribuido, anclajes criptográficos en una cadena pública y resguardo de datos sensibles en dominios privados— permite anticipar beneficios en cuatro frentes: (a) probidad y trazabilidad; (b) eficiencia del control y la auditoría; (c) gobernanza de datos e interoperabilidad; y (d) confianza ciudadana y rendición de cuentas. Se trata de una intervención orientada a resolver problemas prácticos de opacidad, manipulación documental y altos costos de verificación.

El beneficio estructural radica en desplazar parte del aseguramiento desde controles ex post hacia garantías ex ante incorporadas en el diseño del sistema. Ello introduce verificabilidad técnica de los registros, reduce asimetrías de información entre actores y acorta tiempos de conciliación y auditoría. En el resumen del proyecto, estos efectos se sintetizan como capacidad de reducir tiempos y costos de auditoría, fortalecer mecanismos de fiscalización externa y ciudadana y ofrecer un modelo replicable en otras instituciones del Estado (p. 2). La Figura 73 presenta la teoría del cambio de la intervención, explicitando la lógica causal que vincula insumos, actividades, productos, resultados de corto y mediano plazo e impacto esperado. Este esquema facilita evaluar la coherencia interna del proyecto y ubicar los KPI propuestos dentro de una narrativa de transformación institucional.

Figura 73*Teoría del cambio de la intervención*

Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. Relación causal entre insumos, actividades, productos, resultados (12-18 meses) e impacto; los KPI propuestos se corresponden con la Tabla 68.

En términos operativos, los beneficios esperados pueden agruparse así:

Probidad, trazabilidad e inmutabilidad. La cadena de bloques genera evidencias criptográficas (hash, sellado temporal y encadenamiento) que incrementan el costo de la manipulación y permiten detectar alteraciones, reforzando la integridad de expedientes y asientos contables.

Eficiencia del control y la auditoría. La verificación por terceros —a partir de anclajes públicos y “recibos” criptográficos— reduce pruebas repetitivas, muestreos extensos y conciliaciones interorganizacionales, además de acortar el ciclo de auditoría y mejorar la focalización de hallazgos.

Gobernanza de datos e interoperabilidad. La separación entre “dato” y “compromiso del dato” (hash) permite compartir evidencias de integridad sin exponer información sensible, mediante estándares de eventos que facilitan integraciones entre organismos.

Transparencia activa y confianza ciudadana. La publicación verificable de evidencias y la trazabilidad de actuaciones refuerzan la rendición de cuentas y habilitan mecanismos de control externo y social más oportunos.

Para orientar la evaluación, se proponen indicadores y metas tentativas (12–18 meses) coherentes con un enfoque de investigación aplicada y evaluación de resultados. La Tabla 68 operacionaliza los beneficios esperados de la intervención en indicadores clave de desempeño, con sus respectivas líneas base, metas y horizontes de evaluación, permitiendo pasar de afirmaciones conceptuales a métricas verificables.

En conjunto, los beneficios esperados combinan efectos técnicos (inmutabilidad, verificabilidad), organizacionales (reducción de tiempos y costos de verificación, mejor gobernanza de datos) y públicos (transparencia y control ciudadano). Ello alinea la intervención con una lógica de solución de problemas concretos en la administración pública y con un estándar de evidencia verificable congruente con la racionalidad científica.

Tabla 68*Beneficios esperados e indicadores clave de desempeño (KPI)*

Beneficio	Indicador (KPI)	Línea base (LB)	Meta (M) 12–18 meses	Método de evaluación
Integridad de registros	% de expedientes con inconsistencias detectadas en auditoría	X%	X–(30–50%)	Revisión de hallazgos y trazas hash
Trazabilidad	% de actuaciones con sello de tiempo y hash verificable	0–Y%	≥ 95%	Muestreo y verificación criptográfica
Eficiencia de auditoría	Tiempo medio de conciliación interáreas (días)	T ₀	T ₀ –(30–40%)	Cronometría de procesos y logs
Costo de verificación	Horas-hombre por auditoría sustantiva	H ₀	H ₀ –(20–35%)	Planillas de horas y alcance de pruebas
Transparencia	Latencia de publicación de evidencias (días)	L ₀	L ₀ –(40–60%)	Tiempos de publicación de anclajes
Control externo	N.º de observaciones reiteradas por período	O ₀	O ₀ –(20–30%)	Comparación de informes
Confianza	Variación en índice de satisfacción/ confianza	n/d	+10–15%	Encuesta breve a usuarios/ciudadanía
Interoperabilidad	Integraciones activas con otras áreas/organismos	n	n + 2–4	Registro de integraciones y APIs
Cumplimiento	% de procesos críticos con evidencia inmutable	Z%	≥ 90%	Matriz de criticidad y muestreo

Nota. Elaboración propia. Los indicadores (KPI) se calibrarán con línea base institucional y se evaluarán a 12–18 meses; los rangos de meta son orientativos y deben ajustarse tras el piloto. Definiciones: LB = línea

base; M = meta; T_0 = tiempo medio inicial; H_0 = horas-hombre iniciales; L_0 = latencia inicial; O_0 = observaciones iniciales; n/d = no disponible; p95 = percentil 95. La “verificación criptográfica” refiere a comprobación de hash, sello de tiempo y pruebas de inclusión en anclajes públicos.

7.3 Limitaciones del enfoque propuesto

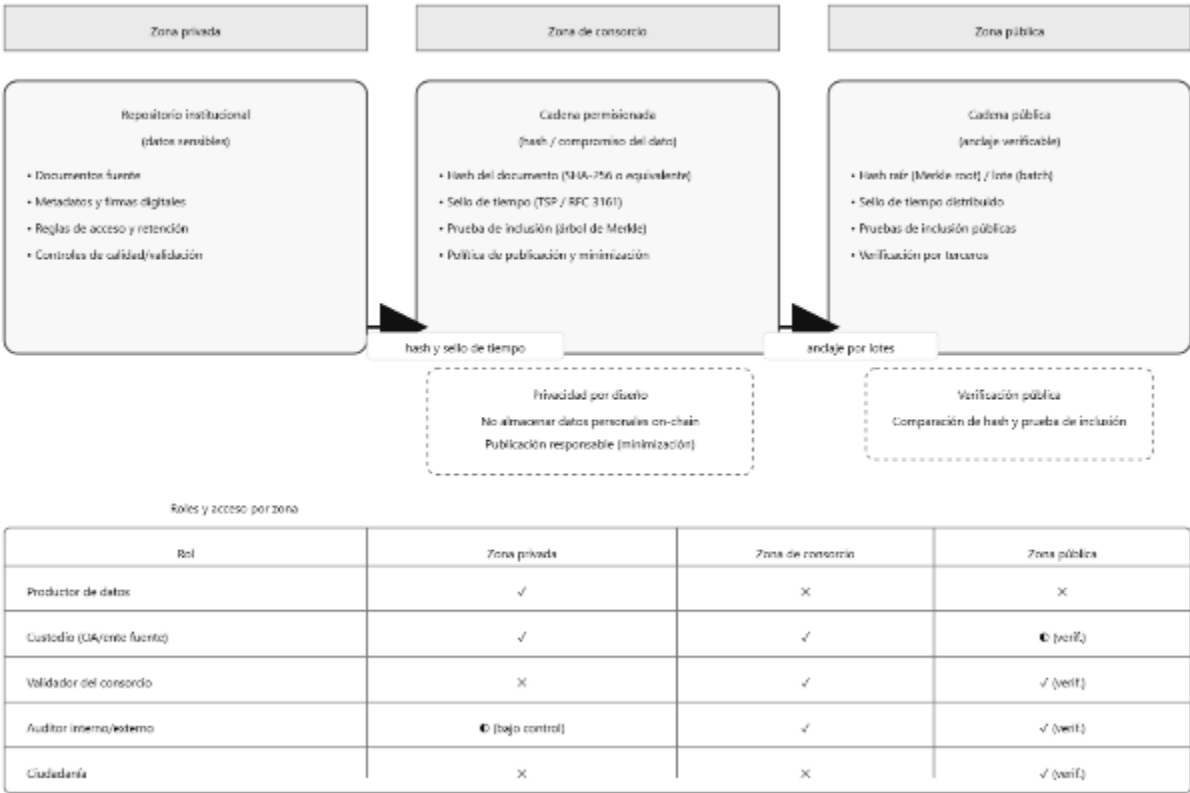
La adopción de una arquitectura blockchain híbrida en la gestión pública presenta limitaciones que deben asumirse como condiciones de diseño y de política institucional. Estas limitaciones pueden agruparse en cinco ejes: (a) marco jurídico–regulatorio y privacidad; (b) gobernanza del consorcio y control interno; (c) calidad, semántica e interoperabilidad de los datos; (d) desempeño, latencia y costos operativos; y (e) madurez organizacional y capacidades profesionales.

Marco jurídico–regulatorio y privacidad. La compatibilidad con el régimen de protección de datos exige minimizar la presencia de datos personales en la cadena y garantizar que los contenidos identificables permanezcan bajo control institucional. Las directrices europeas —adoptadas aquí como “mejor práctica”— recomiendan evaluar el modelo técnico y evitar el almacenamiento de datos personales on-chain, privilegiando evidencias (hashes, punteros o compromisos) y manteniendo verificadores off-chain con alta confidencialidad (EDPB, 2025). En el diseño propuesto esto se traduce en privacidad desde el diseño, EIPD y publicación responsable, con respaldo legal de la firma digital para la validez probatoria del documento fuente (Ley 25.506, 2001; AAIP & URCDP, 2020; Ley 25.326, 2000).

Los responsables del tratamiento deben evaluar la tecnología y el modelo de blockchain que mejor se adapte a sus necesidades [...]. En general, no es recomendable almacenar datos personales en la blockchain [...]. Siempre que sea necesario almacenar datos personales en la blockchain, es preferible almacenar datos destinados a funcionar como prueba de existencia (por ejemplo, punteros, compromisos criptográficos o hashes con clave), manteniendo los datos utilizados para verificar la prueba fuera de la blockchain y garantizando un alto nivel de confidencialidad. (EDPB, 2025, pp. 10–12)

La Figura 74 sintetiza la arquitectura de privacidad on/off-chain propuesta para el piloto. El esquema muestra la separación entre datos sensibles y evidencias criptográficas, los componentes que intervienen en cada dominio y la distribución de accesos según rol, con el objetivo de compatibilizar verificabilidad pública y protección de datos personales.

Figura 74
Arquitectura de privacidad on/off-chain



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. Esquema de separación dato/compromiso: los datos sensibles permanecen en el repositorio institucional; la cadena permissionada almacena hash/compromiso y sellos de tiempo; la cadena pública conserva el anclaje para verificación por terceros. Se aplica minimización y publicación responsable. La matriz resume el acceso por roles a cada zona.

Adicionalmente, la evolución normativa sobre acceso a la información exige cautelas: la transparencia debe aumentar sin generar nuevas barreras de acceso, por lo que la política de publicación de evidencias debe armonizarse con las disposiciones recientes (Ley 27.275, 2016; Decreto 780/2024, 2024).

Gobernanza del consorcio y control interno. En redes multi-actor (por ejemplo, OA, AGN, SIGEN y Hacienda) el riesgo central radica en la ambigüedad de las reglas de membresía, quórum de cambio, administración de claves y auditoría de operaciones críticas. Sin una gobernanza explícita, la trazabilidad puede degradarse y la rendición de cuentas diluirse (Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; COSO, 2013; INTOSAI, 2013).

Calidad, semántica e interoperabilidad. La inmutabilidad no corrige errores de origen; los fija. Sin catálogos gobernados, validaciones y trazabilidad de transformaciones, la cadena consolida inconsistencias.

Con normalización e interoperabilidad, en cambio, se convierte en un “amplificador de confianza” (BID, 2020; COSO, 2013; INTOSAI, 2013). La literatura aplicada subraya que, si no hay semántica compartida, reglas de publicación y capacidades instaladas, la infraestructura distribuida no resuelve el problema de calidad de datos.

Desempeño, latencia y costos. En un consorcio permissionado con anclaje público, la finalidad rápida para cierres contables convive con ventanas de consolidación para el anclaje. El diseño plantea como objetivo una latencia documento→anclaje ≤ 24 h (promedio mensual), con tolerancia a fallas limitada por el número de validadores (por ejemplo, 5 validadores toleran una caída sin interrumpir consenso). Estos parámetros deben demostrarse empíricamente antes del escalado (NIST, 2018). En costos directos, el TCO referencial del piloto (12 meses) se ubica en torno a USD 36.000–48.000, con rubros críticos en HSM/KMS, observabilidad y fees de anclaje (política de batching y fee-cap). La indisponibilidad o congestión de la red pública añade riesgo operativo y requiere multianclaje y reintentos (NIST, 2018; ISO/IEC, 2022; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020).

Madurez organizacional y capacidades. La evidencia comparada muestra una tensión entre beneficios esperados y fricciones de adopción. Sin catálogos normalizados, procedimientos de cambio y responsabilidades trazables, la inmutabilidad puede fijar inconsistencias y desplazar el problema (González González, 2023; Luna González Becerril, 2020; Foro Económico Mundial & Banco Interamericano de Desarrollo, 2020; INTOSAI, 2013). La formación contable y de auditoría resulta decisiva para traducir artefactos técnicos (hashes, pruebas de inclusión, logs) en evidencia probatoria y sostener auditoría continua.

Entre las limitaciones más relevantes del enfoque propuesto se encuentra el hecho de que su factibilidad no depende exclusivamente de la consistencia técnica de la arquitectura diseñada, sino también de condiciones institucionales, organizacionales y presupuestarias cuya estabilidad no puede darse por supuesta en la práctica. En particular, la disponibilidad sostenida de financiamiento, la existencia de capacidades especializadas, la madurez de los procesos de datos, la eventual dependencia de proveedores tecnológicos y la estabilidad de las decisiones político-administrativas inciden de manera directa en la posibilidad de sostener, ampliar o replicar el piloto. Por ello, los beneficios esperados deben leerse como potencialidades condicionadas por el contexto real de implementación, y no como efectos automáticos derivados de la sola adopción tecnológica.

Estas limitaciones no anulan la utilidad pública de la propuesta, pero definen condiciones de éxito: gobernanza clara y auditable, mapeo legal on/off-chain, calidad y semántica de datos adecuadas, métricas de latencia y finalidad demostradas y capacidades profesionales suficientes para operar y auditar el sistema. En ausencia de estas condiciones, los límites de adopción pueden superar los beneficios.

7.4 Escalabilidad y replicabilidad

La escalabilidad del enfoque propuesto se analiza en dos planos complementarios. En el plano técnico, refiere a la capacidad de la red para absorber mayor volumen de transacciones, nodos y datos con niveles controlados de latencia y costos. En el plano organizacional, alude a la capacidad institucional para sostener procesos, gobierno de datos, seguridad y auditoría a medida que se incorporan nuevas áreas y organismos. La replicabilidad, por su parte, alude a la posibilidad de reproducir el diseño en otros contextos con resultados comparables, preservando las garantías de integridad, trazabilidad y control que justifican la intervención.

En la arquitectura híbrida definida —libro mayor distribuido con resguardo de datos sensibles off-chain y anclaje criptográfico en una cadena pública— la inmutabilidad verificable se preserva aun cuando crece el número de procesos y actores, siempre que se mantengan las condiciones de diseño y operación. La validez externa y la generalización de resultados exigen que el piloto demuestre, con métricas observables, que el desempeño y las garantías de integridad se sostienen cuando aumentan casos de uso, volumen documental y cantidad de validadores; en caso contrario, los hallazgos no serían extrapolables a nuevas dependencias.

La estrategia de escalabilidad técnica se apoya en tres palancas: (a) separación dato/compromiso (el dato permanece bajo control institucional y la prueba de integridad viaja como hash y sello de tiempo); (b) anclaje por lotes con ventanas configurables (batching), que permite crecer en volumen sin multiplicar costos unitarios; y (c) horizontalidad de validadores en consorcio (agregar nodos para resiliencia y throughput respetando reglas de gobernanza y quórum). A ello se suman prácticas de observabilidad (métricas de latencia de escritura, tiempo hasta anclaje, tasa de reintentos, almacenamiento por bloque) y gestión de claves alineadas con las exigencias de control interno.

En el plano organizacional, la estrategia de escalado incorpora: (a) catálogos y semántica de datos gobernados; (b) políticas de publicación que separan evidencia pública de contenido sensible; (c) manuales de operación y auditoría que traducen artefactos técnicos (hash, pruebas de inclusión) en evidencia probatoria; y (d) formación de perfiles clave (contabilidad, auditoría, TI y jurídico). La replicabilidad exige, además, plantillas de integración y criterios de aceptación homogéneos entre organismos. La Tabla 69 identifica las principales palancas de escalabilidad y los criterios de replicabilidad de la solución en otros organismos o dominios, vinculando cada palanca con métricas técnicas y de gobernanza.

Tabla 69
Palancas de escalabilidad y criterios de replicabilidad

Eje	Definición operacional	Indicadores	Meta piloto (6–12 meses)	Criterio de replicabilidad
Rendimiento de red	Latencia escritura→anclaje con batching configurable	p95 latencia (min), tasa de reintentos (%)	≤ 24 h promedio; ≤ 5% reintentos	Mismas metas con +50% volumen
Resiliencia	Continuidad ante caída de nodos/servicios	Disponibilidad (%), RTO (min)	≥ 99,5%; RTO ≤ 60	Cumplir con +1 validador agregado
Integridad verificable	Trazas hash y sellos de tiempo auditables	% de actuaciones con evidencia	≥ 95%	Igual o mayor en nueva unidad
Costos unitarios	Costo por anclaje/expediente (USD)	Media y desviación	–30/40% vs. línea base	Estabilidad con +2 casos de uso
Semántica de datos	Catálogos y reglas de validación	% campos regidos por diccionario	≥ 90%	Catálogo replicado sin ambigüedad
Gobernanza	Reglas de membresía/quórum y claves	Cumplimiento de política	100%	Misma política en otro organismo
Auditoría	Procedimientos y evidencias reejecutables	% de pruebas automatizadas	≥ 70%	Reproducción en entorno distinto
Capacidades	Formación y roles críticos cubiertos	% perfiles formados	≥ 80%	Igual cobertura en expansión

Nota. Elaboración propia. Criterios de escalabilidad y replicabilidad medidos con métricas de desempeño y de gobernanza: latencia documento→anclaje (p95), tasa de reintentos, disponibilidad y RTO (tiempo objetivo de recuperación). Definiciones: batching = anclaje por lotes; validador = nodo con rol de consenso; quórum = regla mínima de validación para cambios/actualizaciones. La replicabilidad exige documentar parámetros (consenso, política de anclaje, catálogos semánticos) y reproducir resultados con variaciones toleradas en nuevos contextos.

La hoja de ruta de expansión contempla cuatro etapas:

Escala intrainstitucional (meses 0–6): un área crítica, 2–3 procesos, 3–5 validadores; definición de catálogos y KPI.

Escala interáreas (meses 6–12): incorporación de 2 casos de uso adicionales, sumar validadores e intensificar integraciones y auditoría continua parcial.

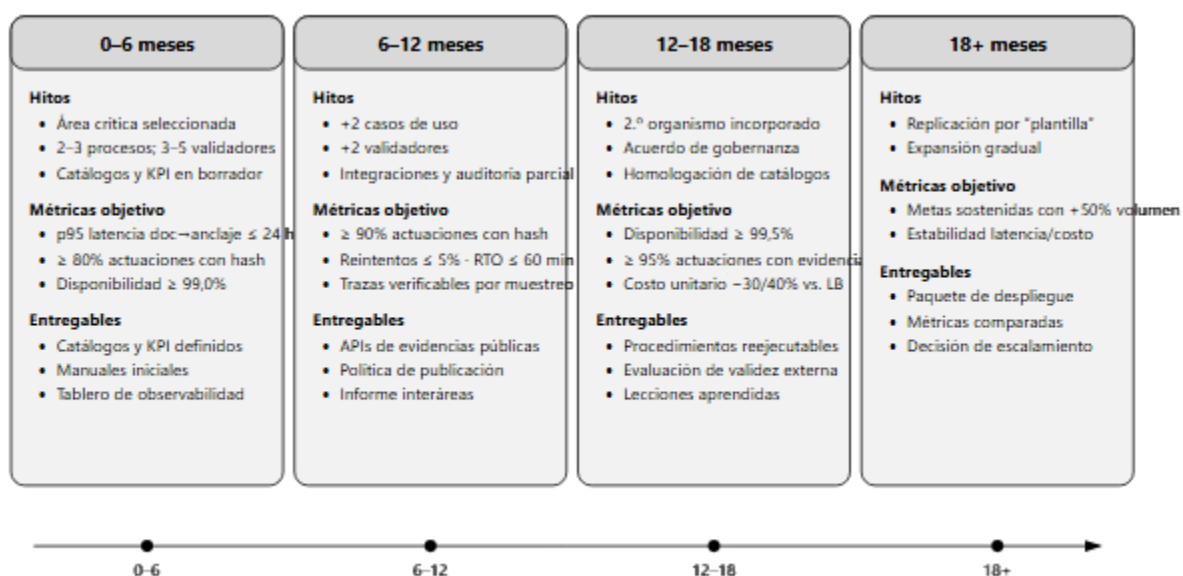
Escala interinstitucional (meses 12–18): incorporación de un segundo organismo, acuerdo de gobernanza y homologación de catálogos.

Replicación (meses 18+): despliegue por “plantilla” con metas de desempeño y calidad de datos predefinidas; evaluación de validez externa (mismas métricas en nuevos contextos).

La Figura 75 representa gráficamente esta hoja de ruta, articulando fases, hitos y entregables, con énfasis en consolidar primero el piloto, luego escalar a nuevas áreas y, finalmente, institucionalizar el modelo como infraestructura compartida en función de las métricas y lecciones aprendidas.

Figura 75

Hoja de ruta de expansión (0–18+ meses)



Nota. Imagen elaborada mediante inteligencia artificial con ChatGPT (OpenAI, 2026), a partir de un prompt elaborado por el autor. Secuencia de despliegue por fases con hitos, métricas objetivo y entregables para evaluar escalabilidad y replicabilidad.

La replicabilidad, en sentido estricto, requiere condiciones iniciales explícitas (versionado del software, parámetros de consenso, políticas de anclaje, catálogos) y criterios de éxito verificables (las mismas métricas deben conducir a conclusiones análogas en otras unidades). Si estas condiciones se documentan y se cumplen, el diseño puede generalizarse sin pérdidas significativas de rendimiento o de

evidencia; de lo contrario, la expansión puede introducir sesgos o heterogeneidades que comprometan la interpretación de resultados.

El modelo es escalable si mantiene latencia, disponibilidad, integridad verificable y costos unitarios dentro de bandas objetivo al crecer en volumen y actores; y es replicable si, en nuevos entornos, reproduce procedimientos, métricas y garantías con variaciones toleradas. Estos criterios derivan de una concepción de la investigación aplicada como práctica sistemática, verificable y falible, que busca resultados útiles y generalizables sin perder el control crítico sobre sus supuestos.

7.5 Alineación con estrategias globales

La intervención propuesta —red blockchain híbrida con resguardo de datos sensibles off-chain y anclaje criptográfico en cadena pública— se alinea con las agendas de integridad, gobierno abierto y transformación digital del sector público. En la Agenda 2030, la arquitectura contribuye a los ODS 16.5, 16.6 y 16.10 al reforzar transparencia, trazabilidad y acceso a la información (Organización de las Naciones Unidas [ONU], 2015). En el plano normativo, la Convención de las Naciones Unidas contra la Corrupción exige registros adecuados, publicidad suficiente y participación para la rendición de cuentas; la separación dato/compromiso y los anclajes verificables fortalecen estas exigencias (Oficina de las Naciones Unidas contra la Droga y el Delito [ONUDD], 2004, arts. 9, 10 y 13). Programáticamente, la Alianza para el Gobierno Abierto estructura sus reformas en torno a transparencia, participación cívica y rendición de cuentas, donde la tecnología actúa como palanca; la propuesta habilita transparencia verificable sin exponer datos personales y soporta control social basado en evidencias públicas (Open Government Partnership [OGP], 2019).

La OCDE promueve sistemas de integridad de “todo el Estado y toda la sociedad” y la transición hacia un sector público digital by design, con datos abiertos, trazables y sujetos a evaluación continua. La inmutabilidad verificable y la gobernanza de identidades y nodos dialogan con estas recomendaciones (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2014, 2017, 2020). En materia de gestión, ISO 37001 (anticorrupción), ISO 37301 (cumplimiento) e ISO/IEC 27001 (seguridad de la información) proporcionan marcos para controles, procedimientos y mejora continua; la segmentación on/off-chain, la política de anclaje y la gestión de claves permiten mapear controles técnicos a cláusulas específicas (International Organization for Standardization [ISO], 2021, 2025; ISO/IEC, 2022). En las prioridades recientes del G20, la integridad pública, la transparencia y la recuperación de activos ocupan un lugar central; la evidencia criptográfica facilita cooperación interinstitucional y forense digital (Grupo de los Veinte [G20], 2024). Finalmente, el enfoque se articula con el paradigma GovTech del Banco Mundial, que enfatiza plataformas compartidas, interoperabilidad y participación ciudadana (Banco Mundial, 2022).

Cada Estado Parte adoptará las medidas necesarias para establecer sistemas adecuados de contratación pública con arreglo a principios de transparencia, competencia y criterios objetivos de adopción de decisiones [...] y tomará medidas para promover la transparencia y la rendición de cuentas en su administración pública. (ONUDD, 2004, art. 9)

La Tabla 70 mapea la intervención propuesta frente a marcos y estrategias globales en materia de integridad, gobierno abierto, transformación digital y GovTech. El objetivo es situar el proyecto en un contexto internacional más amplio y mostrar su coherencia con compromisos y lineamientos de organismos multilaterales.

En conjunto, la intervención capitaliza principios globales para reforzar integridad y control social (ODS, UNCAC, OGP, OCDE, ISO, G20, OEA y GovTech). La convergencia programática se expresa en que la infraestructura de evidencia verificable y gobernanza multi-actor fortalece transparencia y rendición de cuentas en clave de política pública (ONU, 2015; OCDE, 2017; Banco Mundial, 2022).

Tabla 70*Mapa de alineación entre la intervención y estrategias globales*

Marco/estrategia global	Propósito/Principios relevantes	Aporte del enfoque propuesto	Indicadores sugeridos de alineación
ODS 16.5/16.6/16.10 (ONU, 2015)	Reducir corrupción; instituciones eficaces; acceso a información	Evidencias inmutables y públicas (hash-time); trazabilidad de actuaciones; publicación responsable	% actuaciones con hash verificable; latencia de publicación; hallazgos de auditoría sobre integridad
UNCAC (ONUDD, 2004, arts. 9, 10, 13)	Contratación íntegra; gestión financiera; transparencia y participación	Registro distribuido; pruebas de inclusión y anclaje; bitácoras reejecutables	Cobertura de procedimientos críticos con evidencia; % procesos de compras con anclaje por etapa
Valores OGP (OGP, 2019)	Transparencia; participación cívica; rendición de cuentas	Portal de verificación pública; trazas para control social; APIs de evidencias	Nº evidencias verificables; consultas/descargas; reutilización por sociedad civil
Recs. OCDE (OCDE, 2014, 2017, 2020)	Enfoque sistémico; <i>digital by design</i> ; datos abiertos y trazables	Inmutabilidad por diseño; catálogos gobernados; auditoría continua	Autoevaluación de principios OCDE; madurez de gobierno digital
ISO 37001/37301/27001 (ISO, 2021, 2025; ISO/IEC, 2022)	Anticorrupción; cumplimiento; seguridad de la información	Segregación on/off-chain; KMS/HSM; trazas y revisiones	% controles ISO implementados y auditados; residuos de riesgo
G20/ACWG (G20, 2024)	Integridad pública; transparencia; recuperación de activos	Evidencia forense interoperable; cooperación interinstitucional	Casos con colaboración soportada por anclajes y recepción probatoria
IACAC/MESICIC (OEA, 1996)	Prevención, detección, sanción; cooperación regional	Evidencias verificables; cumplimiento de recomendaciones	Recomendaciones atendidas; métricas de cumplimiento regional
GovTech/GTMI (Banco Mundial, 2022)	Plataformas compartidas; servicios digitales; participación	Reutilización de evidencias; interoperabilidad; habilitadores regulatorios	Avance en componentes del GTMI (plataformas, servicios, datos, habilitadores)

Nota. Elaboración propia. Mapa de alineación con marcos ONU/UNCAC, OGP, OCDE, ISO/IEC, G20, OEA y enfoque GovTech. La asociación propuesta es programática y no supone certificación ni cumplimiento automático; debe complementarse con evaluación legal y de políticas públicas propia de cada jurisdicción (ONU, 2015; Oficina de las Naciones Unidas contra la Droga y el Delito [ONUDD], 2004; Open Government Partnership [OGP], 2019; Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2014, 2017, 2020; International Organization for Standardization [ISO], 2021, 2025; ISO/IEC, 2022; Grupo de los Veinte [G20], 2024; Organización de los Estados Americanos [OEA], 1996; Banco Mundial, 2022). Abreviaturas: ODS = Objetivos de Desarrollo Sostenible; UNCAC = Convención de las Naciones Unidas contra la Corrupción; OGP = Alianza para el Gobierno Abierto; OCDE = Organización para la Cooperación y el Desarrollo Económicos; ISO/IEC = International Organization for Standardization/International Electrotechnical Commission; G20/ACWG = Grupo de los Veinte/Anti-Corruption Working Group; OEA/IACAC = Organización de los Estados Americanos/Convención Interamericana contra la Corrupción; GTMI = GovTech Maturity Index.

7.6 Conclusiones preliminares

La arquitectura blockchain híbrida desarrollada en este trabajo constituye una respuesta técnicamente consistente y conceptualmente fundada al problema de la integridad, la trazabilidad y la auditabilidad de la evidencia contable en el sector público. Su aporte principal no radica en sustituir los mecanismos tradicionales de registración, control o fiscalización, sino en incorporar una capa adicional de verificabilidad criptográfica capaz de reforzar la cadena de custodia documental, reducir asimetrías de información entre actores y mejorar la posibilidad de reconstruir, de manera objetiva y reproducible, la secuencia de eventos relevantes del ciclo de gestión.

Los resultados analizados en las secciones precedentes permiten sostener que la propuesta desplaza parte del aseguramiento desde controles predominantemente ex post hacia controles incorporados en el propio diseño del sistema. Esta reconfiguración fortalece la consistencia del registro, la trazabilidad de operaciones críticas y la disponibilidad de evidencia verificable para tareas de control interno, auditoría y rendición de cuentas. En esa medida, el valor del modelo no debe interpretarse en términos de automatización aislada, sino como una forma de rediseñar la producción y preservación de evidencia con criterios de integridad, temporalidad verificable y mayor robustez probatoria.

Desde el punto de vista funcional, la propuesta presenta ventajas plausibles en materia de reducción de fricciones de verificación, mejora en la detección de inconsistencias, fortalecimiento de la trazabilidad documental y mayor capacidad de demostración del cumplimiento. La integración entre contratos inteligentes, registros inmutables, hashing documental, anclajes y políticas de acceso permite estructurar un entorno en el cual las operaciones relevantes no solo quedan registradas, sino también vinculadas a

mecanismos de validación y seguimiento medible. En consecuencia, la arquitectura propuesta no se limita a preservar información, sino que organiza condiciones para que esa información pueda ser auditada con mayor consistencia.

El análisis comparado realizado a lo largo del capítulo también permite afirmar que la utilidad de la solución depende menos del recurso tecnológico aislado que de su integración con procesos institucionales, criterios de gobernanza, estándares de calidad de datos y mecanismos de supervisión. Por ello, los hallazgos obtenidos no avalan una lectura determinista de blockchain, sino una interpretación instrumental y situada: la solución agrega valor cuando se articula con procedimientos claros, métricas definidas y una lógica de implementación gradual que permita verificar resultados, ajustar desvíos y preservar la continuidad operativa.

Asimismo, la propuesta muestra condiciones favorables para una expansión progresiva hacia otros procesos u organismos, siempre que esa expansión se realice de manera escalonada, bajo reglas explícitas de gobernanza y con monitoreo continuo de desempeño. La hoja de ruta planteada en el trabajo, junto con los criterios de éxito definidos para el piloto, ofrece una base metodológica razonable para ensayar una adopción controlada, evitando extrapolaciones prematuras o promesas de impacto no validadas.

En suma, el desarrollo efectuado permite concluir que una arquitectura blockchain híbrida como la aquí propuesta puede constituir una mejora relevante en materia de integridad documental, auditabilidad y transparencia verificable en el ámbito público. Su pertinencia surge no solo de la coherencia técnica del diseño, sino también de su alineación con demandas contemporáneas de control trazable, evidencia robusta y rendición de cuentas sustentada en registros verificables. Precisamente por ello, el alcance efectivo de esta contribución debe examinarse a la luz de los factores institucionales, normativos, organizacionales y operativos que condicionan su implementación, cuestión que se aborda en el capítulo siguiente.

Capítulo 9: Factores condicionantes

9.1 Condicionantes institucionales, normativos y operativos

La consistencia técnica de la propuesta no elimina la necesidad de considerar las condiciones que enmarcan su eventual implementación. En trabajos de intervención aplicados al sector público, el valor de una solución no depende exclusivamente de su diseño conceptual o de su sofisticación tecnológica, sino también del conjunto de factores institucionales, jurídicos, organizacionales y operativos que determinan si esa solución puede desplegarse de manera efectiva, legítima y sostenible. En este caso, la arquitectura propuesta presenta potencial para fortalecer la integridad y la auditabilidad de la evidencia contable, pero ese potencial se encuentra condicionado por un entorno que debe ser explicitado para delimitar adecuadamente el alcance del aporte realizado.

Un primer factor condicionante corresponde a la dimensión institucional y de gobernanza. La implementación de una infraestructura de evidencia verificable requiere patrocinio organizacional, definición de responsabilidades y coordinación entre áreas con racionalidades diferentes, entre ellas las técnicas, jurídicas, operativas y de control. Sin una instancia clara de conducción que articule esas perspectivas, establezca prioridades y resuelva tensiones de implementación, la propuesta corre el riesgo de permanecer como diseño técnicamente sólido pero con baja capacidad de institucionalización. La gobernanza, en este sentido, no constituye un complemento accesorio, sino una condición estructural de viabilidad.

Un segundo condicionante se vincula con la calidad e interoperabilidad de los datos de origen. La verificabilidad criptográfica permite asegurar integridad sobre lo registrado, pero no corrige por sí sola inconsistencias semánticas, errores de carga, debilidades de clasificación o problemas heredados de sistemas previos. En consecuencia, la eficacia de la arquitectura propuesta depende de que existan umbrales mínimos de normalización documental, catálogos coherentes, metadatos suficientes y reglas de integración que permitan que la información preservada sea, además de íntegra, útil para la auditoría y el control. Allí reside una distinción central: la tecnología puede robustecer la evidencia, pero no reemplaza la calidad del dato que le da origen.

A ello se suma un condicionante normativo y regulatorio. La incorporación de mecanismos basados en blockchain al tratamiento de evidencia pública debe resultar compatible con exigencias relativas a protección de datos personales, confidencialidad, acceso a la información, conservación documental, firma digital, validez probatoria y responsabilidades administrativas. Por esta razón, la implementación no puede concebirse como una decisión puramente informática. Requiere una evaluación jurídica previa que determine qué información puede registrarse, bajo qué modalidad, con qué grado de exposición y mediante

qué salvaguardas. La arquitectura híbrida propuesta procura atender esta tensión al separar lo que debe preservarse fuera de cadena de aquello que puede ser anclado o verificado criptográficamente, pero esa decisión debe siempre adaptarse al marco normativo aplicable.

Otro factor relevante está dado por las capacidades organizacionales disponibles. La adopción de una solución de este tipo exige competencias técnicas para operar la infraestructura, pero también capacidades funcionales para comprender su lógica de control, monitorear indicadores, administrar identidades, gestionar incidentes y traducir el valor tecnológico a rutinas institucionales concretas. Sin capacitación, apropiación progresiva y redefinición de responsabilidades, incluso una solución bien diseñada puede producir resistencia, usos parciales o dependencias excesivas respecto de proveedores especializados. La dimensión humana y organizacional resulta, por tanto, tan decisiva como la dimensión técnica.

También debe considerarse la dimensión económico-operativa. Aunque el trabajo propone una hoja de ruta gradual, la puesta en marcha de la solución requiere recursos para infraestructura, integración, seguridad, monitoreo, mantenimiento y soporte. Por ello, su conveniencia no puede evaluarse de modo abstracto, sino en relación con la criticidad de los procesos alcanzados, el volumen de evidencia involucrada y la magnitud del beneficio esperado en términos de trazabilidad, capacidad de verificación y fortalecimiento del control. No todos los procesos justifican el mismo nivel de complejidad tecnológica, y una adopción responsable exige distinguir entre ámbitos donde la mejora sería sustantiva y otros donde el costo de implementación podría resultar desproporcionado.

Un condicionante adicional reside en la gobernanza interactoral propia del modelo propuesto. La participación de múltiples actores, la eventual lógica de consorcio, la distribución de permisos, los umbrales de validación y la gestión de claves exigen definiciones precisas sobre roles, atribuciones, controles cruzados y procedimientos de contingencia. Esta dimensión es especialmente sensible porque uno de los fundamentos de la propuesta consiste en distribuir confianza mediante reglas auditables y no mediante opacidades discrecionales. Si esas reglas no son explícitas, la solución perdería parte sustancial de su legitimidad funcional.

Por otra parte, la escalabilidad y transferibilidad del diseño no deben asumirse de manera lineal. Aunque la arquitectura fue concebida con vocación de replicabilidad, cada organismo público presenta distintos niveles de madurez digital, diversidad de procesos, culturas de control y restricciones normativas. En consecuencia, la expansión del modelo debe entenderse como adaptación situada y progresiva, no como simple réplica técnica. La misma solución puede requerir ajustes significativos según el contexto institucional en el que se aplique.

Finalmente, corresponde señalar un condicionante metodológico y empírico. El presente trabajo desarrolla una propuesta de intervención fundada, con arquitectura definida, indicadores previstos y

criterios de éxito explicitados, pero la validación plena de sus efectos requiere instancias posteriores de pilotaje, medición longitudinal y contraste con líneas de base operativas. Esto implica que el alcance del estudio consiste en demostrar viabilidad argumentada y diseño estructurado, no en afirmar una implementación concluida con resultados ya estabilizados. Lejos de debilitar la propuesta, esta delimitación permite ubicarla con mayor rigor dentro de sus posibilidades reales de desarrollo.

En síntesis, los factores condicionantes identificados no anulan la pertinencia del modelo, sino que delimitan el marco dentro del cual su adopción podría traducirse en valor público verificable. La relevancia de la propuesta reside, precisamente, en mostrar que el uso de blockchain en la gestión pública solo resulta defendible cuando se integra con legalidad, gobernanza, calidad de datos, capacidades institucionales y evaluación medible. A partir de esta delimitación, es posible avanzar hacia una discusión final sobre el aporte del trabajo y sobre el modo en que sus resultados responden al problema y a los objetivos planteados.

9.2 Viabilidad institucional, sostenibilidad y dependencia tecnológica

La viabilidad efectiva de un piloto de estas características en el sector público argentino no depende únicamente de su solidez técnica ni del valor conceptual del modelo propuesto, sino de la convergencia de condiciones institucionales, presupuestarias y organizacionales que, en la práctica, suelen resultar más difíciles de estabilizar que la propia tecnología. En particular, la implementación requiere patrocinio político-administrativo sostenido, coordinación entre áreas técnicas, jurídicas y operativas, disponibilidad de perfiles especializados, calidad y disciplina en la gestión de datos, y una capacidad mínima de gobernanza para sostener reglas de operación, custodia, auditoría y gestión del cambio. En ausencia de estas condiciones, incluso una arquitectura técnicamente consistente podría quedar reducida a una experiencia acotada, sin posibilidad real de institucionalización.

A ello se suma una dimensión de sostenibilidad que debe ser considerada con especial cautela. Aunque el piloto pueda presentarse con costos acotados en una etapa inicial, su continuidad en el tiempo podría verse tensionada por gastos recurrentes de mantenimiento, soporte, monitoreo, seguridad, actualización tecnológica, capacitación y eventual ampliación de infraestructura. De igual modo, una dependencia excesiva de proveedores tecnológicos, plataformas de nube o servicios especializados de custodia y observabilidad podría generar rigideces, costos de salida elevados o pérdida de autonomía institucional. Finalmente, en escenarios de alternancia política, cambios de gestión o reformulación de prioridades públicas, el proyecto podría ralentizarse, redefinirse o discontinuarse no por una falla técnica intrínseca, sino por la falta de decisión institucional para sostenerlo en el tiempo.

En consecuencia, la factibilidad del piloto debe entenderse como una factibilidad condicionada. Desde el punto de vista técnico, la propuesta resulta plausible y coherente con el estado del arte relevado;

sin embargo, su traducción en una experiencia institucional sostenible depende de variables de gobernanza, financiamiento, capacidades organizacionales y continuidad estratégica que exceden el diseño tecnológico en sentido estricto. Incorporar esta perspectiva permite situar la propuesta en escenarios más realistas de implementación y fortalece su valor como intervención profesional contextualizada.

Conclusiones

El desarrollo realizado a lo largo de esta investigación permite sostener que la aplicación de una arquitectura blockchain híbrida al tratamiento de evidencia contable pública constituye una alternativa plausible para fortalecer la integridad documental, la trazabilidad de operaciones y la auditabilidad de procesos sensibles de gestión. El aporte central del trabajo no consiste en postular una sustitución de los mecanismos clásicos de control, sino en demostrar que es posible reconfigurar la forma en que la evidencia se registra, se preserva y se verifica, incorporando mecanismos criptográficos y reglas de gobernanza que refuercen la capacidad institucional de demostrar cumplimiento, reconstruir decisiones y mejorar la rendición de cuentas.

La contribución del estudio adquiere relevancia en la medida en que traslada discusiones teóricas sobre blockchain, contabilidad pública, auditoría y transparencia hacia una propuesta aplicada al contexto estatal, con delimitación institucional, arquitectura funcional, métricas de evaluación y criterios de implementación. En ese pasaje de lo conceptual a lo operativo radica uno de sus principales méritos: el trabajo no se limita a describir potencialidades generales de una tecnología emergente, sino que formula una intervención concreta orientada a problemas verificables de integridad, control y custodia de evidencia en el ámbito público.

La discusión crítica desarrollada permite, al mismo tiempo, evitar una lectura tecnodeterminista. Blockchain no produce por sí misma transparencia, confianza ni integridad institucional. Tales atributos dependen de la calidad de los datos, de la claridad de las reglas, de la existencia de marcos normativos adecuados, de la capacidad organizacional para operar la solución y de la voluntad institucional de insertar la tecnología en procedimientos de control efectivos. En este punto, el trabajo muestra que la utilidad de la arquitectura propuesta no reside en una promesa abstracta de innovación, sino en su posibilidad de funcionar como infraestructura de evidencia verificable dentro de un ecosistema de decisiones, responsabilidades y controles.

Bajo esa perspectiva, la trazabilidad entre problema, objetivos y resultados puede reconstruirse de manera consistente. El problema planteado al inicio del trabajo se vinculó con las limitaciones de los esquemas tradicionales para asegurar integridad, trazabilidad y auditabilidad suficientes sobre evidencia crítica del ciclo de gestión pública. Frente a ello, el primer objetivo específico, referido a la formulación de una arquitectura blockchain híbrida aplicable al caso, encuentra respaldo en el diseño funcional y de

despliegue desarrollado en el capítulo 5 y en su operacionalización posterior, así como en la definición de metas de diseño asociadas a latencia de anclaje y cobertura de hashing, concebidas como umbrales de referencia para el funcionamiento reproducible y previstas para su medición empírica en la etapa de piloto.

En la misma línea, el objetivo orientado a especificar módulos funcionales para contabilidad, auditoría y publicación quedó materializado en la desagregación modular de la solución, en los casos de uso construidos y en la incorporación de políticas de protección de la información y control de accesos, elementos que permiten vincular la arquitectura propuesta con funciones concretas de registración, verificación y exposición controlada de evidencia. Esa formulación se articula, además, con criterios operativos asociados a integraciones trazables y a verificaciones reproducibles, lo que otorga densidad empírica a una definición que, de otro modo, podría haber permanecido en un plano meramente declarativo.

Por su parte, el objetivo relativo a la especificación de contratos inteligentes para automatizar controles del gasto se refleja en el desarrollo del esquema de eventos, validaciones y reglas de negocio presentado en el trabajo. En esta instancia de diseño, su cumplimiento se sostiene en la posibilidad prevista de reejecutar controles, preservar logs de auditoría y verificar criptográficamente que determinadas reglas operen de forma consistente sobre la secuencia registrada. De este modo, la automatización propuesta no aparece como una simplificación informática, sino como un mecanismo de fortalecimiento del control interno tecnológico, cuya verificación empírica corresponde a la etapa de piloto.

El objetivo referido al establecimiento de criterios e indicadores medibles de impacto institucional también puede considerarse alcanzado en el plano del diseño y de la evaluación prevista, en tanto el trabajo definió instrumentos, umbrales de desempeño, metas de seguimiento y periodicidades de medición que permiten observar, con criterios explícitos, variables vinculadas a latencia, cobertura, desempeño y éxito del piloto. Esta dimensión resulta especialmente relevante porque transforma la trazabilidad y la auditabilidad en resultados susceptibles de medición, en lugar de presentarlas como atributos genéricos o aspiracionales.

A su vez, el objetivo vinculado con la participación ciudadana y los incentivos encuentra expresión en el módulo correspondiente, en la definición de métricas de involucramiento y control social y en la previsión de variables tales como aportes ciudadanos, revisiones públicas y resolución de observaciones. Esto permite afirmar que la propuesta no reduce la transparencia a una publicación pasiva de información, sino que la concibe como apertura a formas controladas y medibles de interacción, supervisión y retroalimentación pública.

Considerados en conjunto, estos resultados permiten sostener que el trabajo responde al problema formulado y desarrolla los objetivos específicos de manera coherente con una lógica de intervención académicamente fundada. Esa coherencia no debe leerse como cierre definitivo del debate, sino como demostración de que existe un camino metodológicamente defendible para trasladar principios de

verificabilidad criptográfica y gobernanza trazable al campo de la contabilidad pública. Precisamente por ello, el valor de la propuesta reside tanto en lo que diseña como en el criterio con que delimita sus condiciones de posibilidad.

El trabajo se circunscribe a la fase de diseño, esto es, la arquitectura, la especificación funcional, los contratos inteligentes y el esquema de evaluación quedan formulados como propuesta de referencia, mientras que la implementación, el despliegue y la validación empírica de los indicadores propuestos se reservan para una etapa de piloto. Esta delimitación está orientada a establecer condiciones verificables y replicables antes de comprometer recursos institucionales en un despliegue operativo.

En definitiva, la tesis contribuye a desplazar la discusión sobre blockchain en la gestión pública desde formulaciones abstractas o celebratorias hacia un plano más riguroso, en el que la innovación solo resulta significativa cuando puede justificarse por su aporte a la integridad, por su compatibilidad con exigencias jurídicas e institucionales y por su capacidad de producir evidencia verificable sobre los procesos que pretende mejorar. En ese marco, la arquitectura propuesta se presenta como una alternativa fundada, gradual y controlable para fortalecer la confiabilidad de la información pública y ampliar las bases técnicas de la rendición de cuentas.

Trabajos futuros

A partir de las conclusiones, se propone una agenda de trabajos futuros orientada a consolidar la viabilidad técnica, jurídica y organizacional de la solución y a preparar su escalamiento gradual. La selección de líneas prioriza cinco dimensiones complementarias: (a) arquitectura e interoperabilidad con fuentes externas, (b) seguridad, verificación y protección de datos, (c) gobernanza multi-actor y gestión del cambio, (d) evaluación de resultados y sostenibilidad económico-operativa, y (e) encuadre jurídico y validez probatoria. Cada línea se concibe como un tramo de investigación aplicada con objetivos verificables, entregables definidos y horizontes temporales diferenciados (0–3, 3–12 y 12–36 meses), de modo tal que los aprendizajes de etapas tempranas alimenten decisiones de inversión y diseño en las sucesivas.

El criterio de priorización combina impacto esperado en integridad pública, factibilidad técnica y organizacional, dependencias entre tareas y nivel de riesgo residual. La ejecución se apoyará en pilotos controlados, métricas de desempeño (KPIs) y revisiones con “gates” de decisión para autorizar escalamientos. Asimismo, se prevé documentación sistemática de hallazgos y lecciones aprendidas, junto con mecanismos de participación y supervisión externa que fortalezcan la legitimidad del proceso. A continuación, se presentan las líneas propuestas de trabajo.

Interoperabilidad avanzada y oráculos confiables. Diseñar y evaluar mecanismos de oráculo con registro de procedencia, reputación y auditorías periódicas, para integrar fuentes externas (p. ej., sistemas financieros, registros catastrales, proveedores críticos) sin debilitar la cadena de custodia (NIST, 2018; INTOSAI, 2013).

Verificación formal de contratos inteligentes. Incorporar pruebas de seguridad y verificación formal de reglas de negocio críticas para minimizar riesgos de ejecución y ambigüedades en condiciones y sanciones automáticas (ISO, 2022).

Evaluación de impacto en protección de datos (EIPD). Profundizar el análisis de privacidad diferencial, minimización de datos y seudonimización, incluyendo modelos de off-chain seguro y referencia on-chain, con salvaguardas para DPIAs y normativa local.

Gobernanza multi-actor y participación cívica. Experimentar esquemas de gobernanza con órganos de control, sociedad civil y proveedores, usando tableros públicos con metadatos verificables y trazas auditables (OGP, 2019).

Economía del proyecto y sostenibilidad. Medir TCO/ROI en horizontes de 3–5 años, sensibilidad de costos de infraestructura, y potenciales beneficios indirectos (disminución de litigios, tiempos de auditoría), incluyendo análisis de huella energética y sostenibilidad operativa.

Replicabilidad y escalamiento multinivel. Probar la solución en nuevos dominios (por ejemplo, obra pública, subsidios, gestión documental de expedientes) y nuevos niveles de gobierno, ajustando catálogos de datos y taxonomías.

Integración con marcos de integridad. Profundizar alineación con recomendaciones OCDE, guías de control INTOSAI, y métricas del GovTech Maturity Index (GTMI) para mapear avances y brechas comparativas (OCDE, 2020; INTOSAI, 2013; Banco Mundial, 2022).

Gestión del cambio y capacidades. Desarrollar rutas formativas por roles (técnicos, jurídicos, auditoría, operadores) y simuladores de procesos para acelerar la adopción; evaluar impactos culturales y barreras de uso.

Validación empírica con KPIs. Ejecutar pilotos controlados con indicadores de integridad (oportunidad de registro, cobertura de eventos, consistencia on/off-chain, tiempos de auditoría) y diseños cuasi-experimentales para estimar efectos causales.

Marco jurídico y validez probatoria. Profundizar análisis de validez jurídica de la evidencia blockchain, su admisibilidad y cadena de custodia, y los requisitos probatorios en sede administrativa y judicial.

Anexos

Anexo 1: Criterios de Admisibilidad Probatoria de Evidencia Blockchain

Este anexo sistematiza los criterios técnicos y documentales necesarios para que la evidencia sustentada en blockchain resulte jurídicamente utilizable, en complemento con la sección 3.5.10 (Marco legal, validez probatoria y responsabilidad). Se propone un checklist de requisitos mínimos para la admisión de asientos respaldados por blockchain en sede administrativa o judicial, junto con ejemplos de cadena de custodia aplicados a documentos electrónicos y recomendaciones para la conservación y presentación de la evidencia ante auditorías, tribunales u organismos de control.

Requisitos técnicos y documentales

Para que un registro sustentado en blockchain tenga fuerza probatoria, no alcanza con invocar la “inmutabilidad” técnica: es preciso articular la solución con el marco jurídico vigente y con prácticas de gestión de evidencia ya reconocidas.

Firma digital válida del emisor

Cada documento o asiento que ingresa al sistema debe estar firmado digitalmente por el funcionario competente, mediante certificados emitidos por un certificador licenciado conforme a la Ley 25.506. La firma digital permite acreditar identidad del emisor, integridad del contenido y no repudio, con la misma validez jurídica que la firma ológrafa (art. 3, Ley 25.506).

Checklist: verificar que:

- el documento electrónico de origen esté firmado digitalmente;
- el certificado se encuentre vigente y sin revocaciones;
- la plataforma de verificación utilizada sea la prevista por la normativa local.

Sello de tiempo confiable

Los asientos deben incorporar un sello de tiempo emitido por una Autoridad de Sellado de Tiempo (TSA) o mecanismo equivalente, que permita probar la existencia del documento en una fecha y hora determinadas. El estándar RFC 3161 es una referencia usual para este tipo de servicios.

Checklist: confirmar que cada lote de evidencias contables:

- posea un timestamp emitido por una TSA o servicio equivalente;
- conserve el comprobante del sello (token RFC 3161 u otro formato estándar);
- documente zona horaria y fuente de tiempo utilizada.

Integridad mediante hashing y anclaje

La solución debe permitir demostrar que el documento no fue alterado desde su incorporación. Para ello se calcula un hash criptográfico del archivo original y se registra en la blockchain. En el diseño propuesto, los

hashes individuales se agrupan en árboles de Merkle, publicándose en la red la raíz correspondiente y, de manera periódica, anclando esa raíz en una blockchain pública. Cualquier modificación posterior del documento implicaría un hash distinto y, por tanto, una evidencia fácilmente refutable.

Checklist: verificar que:

- para cada documento exista un hash asociado;
- se conserven el algoritmo y la implementación utilizados (p. ej., SHA-256);
- sea posible reconstruir la prueba de inclusión (Merkle proof) y rastrear el anclaje público correspondiente.

Procedimientos de cadena de custodia documentados

La robustez criptográfica no reemplaza a la cadena de custodia. Debe estar documentado quién crea, firma, registra, consulta y extrae la evidencia, así como los controles de acceso aplicados. El procedimiento debe describir, como mínimo:

1. cómo se incorporan documentos al sistema (rol, autorización y punto de entrada);
2. cómo se resguardan (controles de acceso, backups, segregación de ambientes);
3. cómo se preparan los paquetes probatorios para su presentación.

Checklist: disponer de un registro de auditoría que consigne, con trazabilidad temporal:

- creación y firma del documento;
- generación de hash y registro en blockchain;
- accesos relevantes, exportaciones y operaciones de verificación.

Metadatos verificables y contexto jurídico

La evidencia digital debe acompañarse de metadatos suficientes para vincularla con el expediente, acto administrativo o proceso que le da origen. Como mínimo, cada registro debería incluir:

- identificador del documento o expediente;
- identificador del firmante vinculado a su certificado;
- referencia temporal y organizacional (área emisora, tipo de acto).

Checklist: comprobar que los metadatos de cada asiento permiten reconstruir:

- qué documento se respalda;
- quién lo generó y aprobó;
- en qué expediente o actuación se enmarca.

Controles de acceso y autenticidad durante todo el ciclo

Debe acreditarse que solo personal autorizado pudo incorporar, modificar o aprobar la información antes del registro definitivo en blockchain. Esto se logra mediante:

- autenticación robusta y segregación de funciones (emisor, aprobador, auditor);
- políticas de control interno estructuradas (COSO, 2013);

- auditorías periódicas de configuración y acceso.

Checklist: contar con:

- documentación de políticas y matrices de roles;
- evidencia de auditorías de sistemas o actas notariales sobre hashes y procedimientos;
- registros de revocación o rotación de credenciales cuando corresponda.
-

Ejemplo de cadena de custodia probatoria

A modo ilustrativo, se detalla el ciclo de una orden de pago incorporada al sistema:

1. Un funcionario habilitado firma digitalmente la orden de pago en el sistema de gestión documental. El documento adquiere un ID único, incluye sello de tiempo y queda registrado en el expediente correspondiente.
2. El sistema de evidencia genera el hash (por ejemplo, SHA-256) del PDF firmado y arma un manifiesto con: hash, ID del documento, identificador del firmante y sello de tiempo confiable.
3. Este manifiesto se registra en la blockchain permissionada mediante una transacción vinculada a la clave institucional. Los nodos del consorcio validan la transacción y el bloque resultante queda encadenado con su hash al bloque anterior.
4. Periódicamente, se calcula la raíz de Merkle de todas las transacciones del período y se publica en una blockchain pública mediante una transacción de anclaje. Ese anclaje actúa como “notaría” distribuida independiente de los participantes.
5. Ante una auditoría o proceso judicial, la institución presenta:
 - el documento original firmado (verificable con la herramienta oficial de firma digital);
 - el hash recalculado del PDF y su coincidencia con el hash registrado on-chain;
 - la prueba de inclusión en el árbol de Merkle y el bloque donde se almacenó;
 - la transacción de anclaje en la blockchain pública, demostrando la existencia del documento a una fecha determinada;
 - la cadena de custodia interna (quién lo generó, aprobó y administró, con base en logs firmados).

En estas condiciones, un perito o juez puede verificar de forma independiente la integridad y cronología del documento, en línea con los criterios de evidencia “suficiente y apropiada” del estándar ISSAI 100 (INTOSAI, 2013).

Preservación y presentación de la evidencia

Conservación a largo plazo

- Uso de formatos estables para archivo (p. ej., PDF/A).

- Almacenamiento redundante en repositorios con características WORM (Write Once Read Many).
- Preservación de logs de auditoría y evidencias técnicas (hashes, pruebas de inclusión, anclajes) en repositorios protegidos, idealmente también respaldados mediante resúmenes periódicos en blockchain.

Presentación comprensible ante autoridades

La presentación de evidencia blockchain debe acompañarse de explicaciones técnicas traducidas a lenguaje jurídico, mediante informes periciales o técnicos que:

- describan qué es un hash, cómo se calculó y dónde se registró;
- expliquen la relación entre documento, hash, bloque y anclaje;
- indiquen cómo se verificó la correspondencia entre todos esos elementos.

Documentación formal de cadena de custodia

Como buena práctica, se recomienda anexar una cadena de custodia en formato tradicional (acta o documento firmado) que resuma el ciclo de vida de cada evidencia: recepción, firma, cálculo de hash, registro en blockchain y verificaciones realizadas.

Simulacros y pruebas piloto

Antes de enfrentar un caso real, conviene realizar ejercicios internos donde se arme un “paquete probatorio completo” a partir de un documento concreto. Esto permite comprobar que todos los elementos son accesibles y que el personal conoce los pasos a seguir.

Cumplimiento normativo integral

El esquema de evidencia debe armonizar:

- transparencia (Ley 27.275);
- administración financiera y control (Ley 24.156);
- protección de datos personales (Ley 25.326);
- régimen de firma digital (Ley 25.506).

Asimismo, deben existir procedimientos excepcionales para la corrección de errores materiales o fraudes acreditados, documentando cualquier rectificación del registro contable original y sus efectos jurídicos.

En síntesis, cuando la generación de evidencia blockchain se acompaña de firma digital válida, sellado de tiempo confiable, integridad verificable, cadena de custodia documentada, controles organizacionales y cumplimiento normativo, los registros de la red pueden alcanzar una fuerza probatoria equiparable a la de los documentos tradicionales, aportando además trazabilidad técnica y transparencia reforzada.

Anexo 2: Playbooks de Respuesta a Incidentes en la Red Blockchain

Este anexo reúne guías operativas (playbooks) para la respuesta a incidentes críticos que pueden afectar la red blockchain propuesta. Los escenarios contemplados se alinean con los riesgos identificados en el Capítulo 6.8 e incluyen: (1) intentos de fraude o ataque en la red; (2) fuga de datos personales o sensibles; y (3) indisponibilidad de oráculos o servicios externos críticos. Para cada caso se describen mecanismos de detección, pasos de contención, investigación, estructura RACI, objetivos de recuperación (RTO/RPO), comunicaciones y criterios de cierre.

Escenario 1: Intento de fraude o ataque en la red blockchain

Descripción:

Comprende eventos como colusión de validadores para alterar registros, uso indebido de claves privadas, inyección de transacciones no autorizadas o explotación de vulnerabilidades de software (riesgos R1 y R3 del análisis de riesgos).

Detección:

Alertas en el monitoreo de la red (desviaciones en latencias, caídas de nodos, fallas de consenso).

Alarmas en el SIEM relativas a uso anómalo de credenciales o claves privadas.

Detección de firmas inválidas o transacciones que violan reglas de negocio.

Contención inmediata (Responsable: equipo de Arquitectura/SRE):

Activar mecanismo de freno de emergencia (emergency brake) si está disponible: suspensión temporal de incorporación de nuevos bloques o de funciones críticas.

Revocar certificados o claves sospechadas de compromiso.

Aislar nodos comprometedores y conmutar a nodos de respaldo, garantizando el quorum mínimo para mantener integridad y disponibilidad.

Investigación y análisis (Consulted: Seguridad de la Información y Auditoría interna):

Revisar logs de la blockchain y sistemas asociados para identificar el origen del incidente (usuario, nodo, clave).

Determinar si se trata de error, abuso de privilegios o ataque externo.

Preservar evidencia técnica (hashes, transacciones, timestamps, direcciones involucradas) para análisis forense y eventuales acciones legales.

RACI:

Responsable: Arquitecto Blockchain / SRE (contención y análisis técnico).

Accountable: Dirección de Proyecto y Comité de Gobernanza de la red.

Consulted: CISO, Auditoría interna, Asesoría Legal.

Informed: Miembros del consorcio y alta dirección de las entidades participantes.

Comunicación:

Notificación interna inmediata al Comité de Crisis de TI y al Comité de Gobernanza.

En caso de impacto potencial hacia la ciudadanía o terceros, preparación de comunicados oficiales coordinados con Asuntos Legales y Comunicación Institucional.

Evaluación de la necesidad de informar a organismos de control y, si corresponde, al Poder Judicial.

RTO/RPO:

RTO objetivo: reestablecer un estado seguro de la red en un plazo acotado (por ejemplo, ≤ 2 horas desde la detección), ya sea mediante aislamiento de nodos, parche de software o cambios de configuración controlados.

RPO objetivo: 0 pérdida de transacciones válidas; cualquier operación legítima afectada debe ser recuperable y reintroducida.

Criterios de cierre:

Vulnerabilidad o vector de ataque identificado y corregido.

Red operando con quorum suficiente y validadores confiables.

Integridad de datos verificada mediante recalcule de hashes y contraste con anclajes.

Informe post-mortem aprobado por la Dirección OA y compartido con el consorcio, incluyendo causas raíz, impacto y medidas correctivas.

Implementación de acciones de mejora (rotación de claves, refuerzo de monitoreo, ajustes de configuración, capacitación).

Escenario 2: Fuga de datos personales o sensibles**Descripción:**

Situación en la que información protegida por la Ley 25.326 u otra normativa de confidencialidad se ve expuesta, ya sea porque datos que debían mantenerse off-chain aparecen en metadatos públicos, o porque un repositorio off-chain es accedido indebidamente (riesgo R5).

Detección:

Reportes de usuarios o terceros que detectan datos sensibles visibles en exploradores públicos.

Alertas de soluciones de Data Loss Prevention (DLP) o SIEM ante volúmenes inusuales de exportación.

Controles periódicos de calidad de datos que identifiquen campos con datos personales en ubicaciones no previstas.

Contención (Responsable: Seguridad de la Información / Datos):

Si la fuga es on-chain, reducir de inmediato la exposición desde interfaces de usuario (por ejemplo, ocultando campos comprometidos en frontends) aun cuando el dato permanezca inmutable en la cadena.

Si la fuga es off-chain, aislar el sistema afectado, bloquear accesos y forzar cambio de credenciales.

Evaluar necesidad de despublicar datasets o desindexar recursos expuestos.

Notificación y aspectos legales (Accountable: DPO y Dirección OA):

Evaluar severidad e impacto sobre los titulares de datos.

Preparar, de ser necesario, notificación a la autoridad de protección de datos (AAIP) y a los afectados, aplicando principios de responsabilidad proactiva.

Coordinar comunicaciones internas y externas con Asesoría Legal y Comunicación Institucional.

Investigación forense:

Analizar logs de acceso, configuración de sistemas y vectores de entrada.

Determinar si fue resultado de error humano, defecto de diseño o intrusión.

Preservar evidencia técnica para una posible investigación externa o judicial.

RACI:

Responsable: CISO / Responsable de Seguridad de la Información.

Accountable: Delegado de Protección de Datos y Dirección OA.

Consulted: Asesoría Legal, Auditoría interna, Comunicación institucional.

Informed: Comité de Seguridad de la Información, Comité de Gobernanza del consorcio.

RTO/RPO:

RTO: restablecer un estado seguro (sin fuga en curso) en pocas horas (p. ej., < 4 horas).

RPO: objetivo de no perder datos, priorizando la confidencialidad (retirada rápida de publicaciones indebidas y bloqueo de accesos).

Criterios de cierre:

Exposición contenida o neutralizada (tanto on-chain a nivel de interfaces como off-chain en repositorios).

Vulnerabilidades corregidas y controles mejorados (validaciones, clasificación de datos, reglas de publicación).

Notificaciones requeridas completadas y documentadas.

Informe de cierre firmado por el DPO, con lecciones aprendidas e incorporación de medidas preventivas adicionales.

Escenario 3: Caída de oráculos o servicios externos críticos

Descripción:

Impacta a servicios de los que depende la solución, como redes públicas para anclajes, proveedores de tiempo confiable u otros sistemas auxiliares (riesgo R2). Ejemplos: indisponibilidad de la red pública utilizada para anclajes o caída de un servicio externo de identidad.

Detección:

Alertas en el monitoreo de SLA (p. ej., anclajes que exceden los tiempos máximos previstos).

Alarmas de fallos repetidos en llamadas a APIs externas.

Notificaciones del propio proveedor del servicio.

Contención (Responsable: DevOps/SRE):

Activar procedimientos de contingencia definidos en el diseño (Cap. 6.8.4):

- anclaje diferido cuando la red pública está congestionada;
- uso temporal de una red alternativa preconfigurada;
- conmutación a fuentes de datos secundarias cuando un oráculo de información cae.

Informar a las áreas usuarias sobre la degradación funcional (por ejemplo, demoras en anclajes sin pérdida de verificabilidad final).

RACI:

Responsable: Ingeniero DevOps/SRE de guardia.

Accountable: Dirección de TI / Dirección de Proyecto.

Consulted: Arquitecto Blockchain, Equipo de Datos.

Informed: áreas usuarias relevantes y Comité de Gobernanza.

Continuidad y objetivos:

Definir ventanas de tolerancia para cada servicio crítico (p. ej., anclajes pueden diferirse hasta 24 horas sin comprometer verificabilidad).

RTO: restablecer el uso normal del oráculo dentro de la ventana de tolerancia; si no es posible, escalar a plan de failover.

RPO: no perder eventos; mantener en cola los hashes o transacciones pendientes.

Plan de failover y recuperación:

Cambiar temporalmente el destino de anclajes a una segunda red pública prevista en el diseño.

Habilitar mecanismos alternativos de autenticación en caso de caída de un servicio de identidad externo.

Documentar íntegramente los cambios realizados en el registro de cambios off-chain.

Criterios de cierre:

Servicio externo restablecido o reemplazado de forma estable.

Procesamiento de todos los eventos pendientes sin pérdida de integridad.

Reversión controlada de configuraciones temporales o adopción permanente si se justifica.

Informe del incidente, impacto y correcciones, con propuestas de mejora de resiliencia (por ejemplo, incorporación de un tercer oráculo o automatización adicional del failover).

Anexo 3: Modelo Energético y Huella Operativa de la Solución

Este anexo presenta una estimación del consumo energético y la huella operativa de la plataforma blockchain propuesta, tanto en términos ambientales (energía y emisiones) como económicos (costos). Complementa el análisis de infraestructura y costos del Capítulo 6.4, detallando supuestos por ambiente (desarrollo, pruebas, producción), proyección de costos energéticos anuales y medidas previstas para mejorar la eficiencia, en línea con buenas prácticas de TI sustentable.

1. Supuestos de infraestructura y consumo

En operación de producción, la red blockchain contempla:

- 5 nodos validadores principales (uno por cada organismo del consorcio);
- Nodos observadores/ligeros para APIs;
- Infraestructura auxiliar (servidor de monitoreo, HSM para llaves, servidor de analytics/ETL);
- Ambientes reducidos de Desarrollo (Dev) y Pruebas (QA/Staging).

La siguiente tabla resume la estimación de consumo:

Dev: ~1,5 kW en horas pico (≈ 13.000 kWh/año).

QA/Staging: ~2 kW (≈ 17.500 kWh/año).

Producción: ~4,5 kW (≈ 39.500 kWh/año).

Total estimado: ~70.000 kWh/año (~70 MWh), con un costo aproximado de US\$ 7.000 anuales suponiendo tarifa de US\$ 0,10/kWh.

Para ofrecer contexto, el consumo anual estimado es comparable al de un conjunto reducido de hogares y varias órdenes de magnitud menor que el de redes públicas de prueba de trabajo con minería intensiva, dado que la solución se basa en consenso eficiente (p. ej., PoA/PBFT) y un número acotado de nodos.

2. Huella de carbono y métricas asociadas

Asumiendo un factor promedio de ~0,4 kg CO₂/kWh para la matriz eléctrica, la emisión anual estimada sería del orden de 28 toneladas de CO₂. El diseño prevé:

Medir la PUE (Power Usage Effectiveness) del centro de datos que aloja los nodos, con un objetivo $PUE \leq 1,5$, conforme a ISO/IEC 30134-2;

Monitorear el REF (Renewable Energy Factor), buscando que al menos el 50 % de la energía provenga de fuentes renovables (ISO/IEC 30134-3), con meta de incrementarlo progresivamente.

Si se consideran también consumos asociados a enfriamiento e infraestructura de apoyo (PUE ~1,5), el consumo total se ubicaría en torno a 105.000 kWh/año ($\approx$ US\$ 10.500 anuales).

3. Medidas de eficiencia energética

Desde el diseño se incorporan decisiones orientadas a reducir el impacto energético:

Consenso de bajo consumo: el uso de algoritmos de consenso tolerantes a fallas bizantinas (p.ej. variantes PBFT) en redes permissionadas evita la necesidad de prueba de trabajo, reduciendo drásticamente el uso de CPU respecto de esquemas de minería intensiva.

Número de nodos ajustado a necesidades de seguridad: se adopta el mínimo número de validadores compatible con la tolerancia a fallas requerida, evitando proliferación innecesaria de nodos.

Virtualización y contenedores: los componentes se despliegan en contenedores ligeros sobre infraestructura virtualizada, consolidando servicios auxiliares cuando es compatible con los requisitos de seguridad.

Uso de energía renovable: se prioriza la instalación en centros de datos con acuerdos de suministro de energía renovable o esquemas de “energía verde”, buscando incrementar el REF de la infraestructura utilizada.

Aprovechamiento de aceleración criptográfica: se emplean librerías que utilizan instrucciones de CPU específicas para operaciones de hashing y criptografía, reduciendo tiempo de procesamiento por transacción.

Gestión activa de potencia: configuración de perfiles de energía que permitan reducir frecuencias de CPU y apagar componentes en períodos de baja carga, sin afectar la disponibilidad requerida.

Monitoreo ambiental: inclusión de indicadores de consumo, PUE y emisiones estimadas en los tableros de monitoreo, con revisión periódica en el ámbito del comité de gobernanza.

4. Resultados esperados y evolución

Con estos supuestos, el costo energético directo de la plataforma se considera manejable frente al presupuesto TI de las entidades participantes. El consumo por transacción es bajo gracias al número limitado de nodos y a la ausencia de minería. El proyecto prevé:

- Revisar periódicamente el dimensionamiento y la utilización de recursos;

- Aprovechar oportunidades de renovación de hardware y actualización de software para incorporar mejoras de eficiencia;

- Evaluar centralización progresiva de infraestructura en entornos compartidos optimizados (p. ej., nube gubernamental eficiente) si la red se extiende a más organismos.

En términos de políticas públicas, se considera la eventual adopción de marcos de gestión de la energía (como ISO 50001) en el ámbito de TI donde se hospede la solución, integrando la plataforma blockchain en objetivos más amplios de uso responsable de recursos.

Anexo 4: Carta de Gobernanza de la Red Blockchain y Reglas del Consorcio

Este anexo sintetiza los elementos principales de la Carta de Gobernanza de la red blockchain consorcial. El documento define la composición del consorcio, sus mecanismos de toma de decisiones, procesos de cambio on-chain y off-chain, criterios de incorporación y salida de miembros, y mecanismos de resolución de controversias. Su finalidad es proporcionar un marco institucional estable para la operación conjunta de la solución descrita en el Capítulo 5.3.

Composición del consorcio

El consorcio está integrado inicialmente por cuatro entidades:

- Oficina Anticorrupción (OA);
- Auditoría General de la Nación (AGN);
- Sindicatura General de la Nación (SIGEN);
- Secretaría de Hacienda (Ministerio de Economía).

Cada miembro opera un nodo validador y participa en las decisiones de gobernanza. La Carta prevé:

- La incorporación de nuevos miembros mediante un procedimiento específico;
- La figura de observadores, que pueden operar nodos de lectura o acceder a la información sin participar en la validación ni en las decisiones (p.ej., organizaciones de la sociedad civil con convenio).

Quóruns y tipos de decisiones

Se distinguen dos categorías de decisiones:

- Decisiones ordinarias: cuestiones operativas (mantenimientos programados, ajustes menores de parámetros, admisión de observadores). Se aprueban por mayoría simple de los miembros presentes.
- Decisiones extraordinarias: cambios de alto impacto (modificación de contratos críticos, incorporación o expulsión de miembros, cambios sustantivos en el plan de anclaje, reversión excepcional de registros, enmiendas a la propia Carta). Requieren mayoría calificada (por ejemplo, 3/4 de los miembros).

Para incidentes de seguridad graves, se establece un Comité de Crisis integrado por un representante técnico de cada miembro, habilitado a tomar medidas urgentes, que luego deben ser ratificadas por los órganos de gobernanza formales.

Procesos de cambio on-chain

Los cambios a los componentes on-chain (contratos inteligentes, parámetros de consenso, reglas de verificación) se gestionan mediante un contrato de administración con control multiestructura:

- Solo transacciones multi-firma con el umbral definido por el quórum extraordinario pueden aprobar cambios críticos;

- Los cambios aprobados quedan sujetos a un timelock: entran en vigor después de un plazo mínimo (por ejemplo, 48 horas), durante el cual los miembros pueden revisar el código y, si detectan problemas, vetarlos.

De este modo, se asegura trazabilidad entre decisiones de gobernanza y modificaciones técnicas efectivas.

Procesos de cambio off-chain

Las decisiones que afectan políticas, procedimientos o acuerdos de servicio se tramitan mediante el Comité de Gobernanza, integrado por representantes designados (por ejemplo, directores de sistemas o equivalentes). El proceso incluye:

- Circulación previa de propuestas;
- Reunión de deliberación y votación;
- Documentación en actas firmadas.

Cuando las decisiones off-chain requieren ajustes on-chain, el acta correspondiente instruye al equipo técnico para ejecutar el cambio siguiendo el mecanismo descrito en el punto anterior. La Carta prevé reuniones ordinarias periódicas y la posibilidad de convocatorias extraordinarias.

Incorporación de nuevos miembros

Las entidades que deseen incorporarse deberán:

- Presentar solicitud formal al Comité de Gobernanza, describiendo objetivos y aportes esperados;
- Aceptar expresamente los principios y responsabilidades de la Carta;
- Obtener aprobación por unanimidad de los miembros actuales en una reunión extraordinaria.

La incorporación puede ser gradual:

- Ingreso inicial como observador (sin funciones de validación);
- Posterior transición a nodo validador, ajustando en consecuencia los parámetros de consenso (por ejemplo, tolerancia a fallas bizantinas) y revisando el quórum de decisión.

Cada incorporación se formaliza mediante un adendum a la Carta.

Salida de miembros y desactivación de nodos

Se contemplan:

Salidas voluntarias: el miembro notifica con antelación suficiente (p.ej., 60 días) para organizar la desvinculación de su nodo y la reasignación de responsabilidades.

Expulsión por incumplimiento grave: puede proponerse cuando un miembro viola de forma reiterada las reglas de gobernanza o compromete la seguridad de la red. La expulsión requiere decisión extraordinaria con el quórum previsto.

En ambos casos:

Se revocan las credenciales asociadas al nodo saliente;

Se ajusta la configuración de consenso para excluirlo de la validación;

El historial de datos permanece en la red, sujeto a las reglas de archivo y conservación aplicables.

Resolución de conflictos

La Carta establece mecanismos escalonados:

Intento de solución interna en el Comité de Gobernanza;

Recurrir a una instancia de mediación externa (por ejemplo, un organismo de coordinación de políticas digitales);

En caso de controversias técnicas sobre la integridad de datos, posibilidad de auditoría independiente con informe técnico;

Para disputas de naturaleza estrictamente jurídica, recurso a los órganos previstos por el ordenamiento vigente, procurando minimizar la judicialización mediante las etapas previas.

La evidencia registrada en la red se asume vinculante salvo prueba de error o fraude, en coherencia con el diseño de integridad y trazabilidad descripto en el trabajo.

Otras reglas relevantes

Seguridad de nodos: cada miembro debe mantener su nodo conforme a estándares de seguridad acordados. La Carta autoriza al Comité a aislar temporalmente nodos con brechas graves hasta su remediación.

Propiedad y uso de la información: los datos pertenecen al dominio público en la medida en que derivan de funciones estatales, pero su tratamiento debe ajustarse a normas de transparencia y protección de datos personales. Todos los miembros pueden utilizar la información para fines legítimos de control y transparencia.

Financiamiento: los costos de operación y evolución de la red se reparten según criterios acordados (por ejemplo, contribuciones equitativas o esquemas diferenciados documentados en anexos financieros).

Vigencia y revisión: la Carta tiene vigencia indefinida, pero su funcionamiento se revisa regularmente. Las modificaciones se tramitan mediante los mecanismos de decisión extraordinaria ya descritos.

En conjunto, estas reglas buscan asegurar que la operación técnica de la red se desarrolle dentro de un marco institucional claro, previsible y documentado, facilitando la continuidad del proyecto más allá de cambios organizacionales o de autoridades.

Acrónimos

ABAC — Attribute-Based Access Control (Control de Acceso Basado en Atributos).

AGN — Auditoría General de la Nación.

BFA — Blockchain Federal Argentina.

BFT — Byzantine Fault Tolerance (Tolerancia a Fallas Bizantinas).

BID — Banco Interamericano de Desarrollo.

CNE — Comisión Nacional de Energía (Chile).

COSO — Committee of Sponsoring Organizations of the Treadway Commission (Marco de Control Interno).

ERP — Enterprise Resource Planning (Sistema de Planificación de Recursos Empresariales).

ETL — Extract, Transform, Load (Extracción, Transformación y Carga).

EVM — Ethereum Virtual Machine.

G20/ACWG — Grupo de los Veinte / Anti-Corruption Working Group.

GTMI — GovTech Maturity Index.

HSM — Hardware Security Module (Módulo de Seguridad de Hardware).

IAM — Identity and Access Management (Gestión de Identidades y Accesos).

INTOSAI — International Organization of Supreme Audit Institutions (Organización Internacional de EFS).

ISO/IEC — International Organization for Standardization / International Electrotechnical Commission.

ISSAI — International Standards of Supreme Audit Institutions (Normas Internacionales de las EFS).

JSON — JavaScript Object Notation.

JWS — JSON Web Signature.

JWT — JSON Web Token.

KMS — Key Management Service (Servicio de Gestión de Claves).

LACChain — Programa/infraestructura del BID para redes blockchain permissionadas en ALC.

MFA — Multi-Factor Authentication (Autenticación Multifactor).

MPC — Multi-Party Computation (Cómputo Multipartito).

OA — Oficina Anticorrupción (Argentina).

OCDE — Organización para la Cooperación y el Desarrollo Económicos.

ODS — Objetivos de Desarrollo Sostenible.

OEA/IACAC — Organización de los Estados Americanos / Convención Interamericana contra la Corrupción.

OGP — Alianza para el Gobierno Abierto.

ONU — Organización de las Naciones Unidas.

ONUDD — Oficina de las Naciones Unidas contra la Droga y el Delito.

OSCE — Organismo Supervisor de las Contrataciones del Estado (Perú).

PBFT — Practical Byzantine Fault Tolerance.

PDF — Portable Document Format.

PoS — Proof of Stake.

PoW — Proof of Work.

QBFT — Quorum Byzantine Fault Tolerance.

RACI — Responsible, Accountable, Consulted, Informed (matriz de responsabilidades).

RBAC — Role-Based Access Control (Control de Acceso Basado en Roles).

SFC — Superintendencia Financiera de Colombia.

SIDIF — Sistema Integrado de Información Financiera (Argentina).

SIEM — Security Information and Event Management (Gestión de Información y Eventos de Seguridad).

SLO — Service Level Objective (Objetivo de Nivel de Servicio).

SoD — Segregation of Duties (Segregación de funciones).

TCO — Total Cost of Ownership (Costo Total de Propiedad).

TI — Tecnologías de la Información.

UNCAC — Convención de las Naciones Unidas contra la Corrupción.

ZK — Zero-Knowledge (Pruebas de Conocimiento Cero).

Referencias

- Adams, C., Cain, P., Pinkas, D., & Zuccherato, R. (2001). *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (RFC 3161)*. Internet Engineering Task Force. <https://www.rfc-editor.org/rfc/rfc3161>
- Administración Federal de Ingresos Públicos (AFIP). (s. f.). Declaración Jurada Patrimonial Integral (F. 1245/F. 1246) – Presentación en ARCA. AFIP.

- <https://serviciosweb.afip.gob.ar/genericos/guiavirtual/archivos/archivos/Guia%20Virtual%20-%20DJ%20Patrimonial%20Integral.pdf>
- Agencia de Acceso a la Información Pública (AAIP). (2018, 25 de julio). *Resolución 47/2018: Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados y no informatizados* (Anexos I y II). AAIP.
<https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662/texto>
- Agencia de Acceso a la Información Pública (AAIP) & Unidad Reguladora y de Control de Datos Personales (URCDP). (2020, 28 de enero). *Guía de Evaluación de Impacto en la Protección de Datos Personales (EIPD)*. AAIP/URCDP.
https://www.argentina.gob.ar/sites/default/files/guia_final.pdf
- Allende López, M. (2021a). *LACChain framework for permissioned public blockchain networks: Blockchain technology for the common good*. Inter-American Development Bank.
<https://publications.iadb.org/en/lacchain-framework-permissioned-public-blockchain-networks-blockchain-technology-blockchain>
- Allende López, M. (2021b). *LACChain ID framework: A set of recommendations for blockchain-based interoperable and privacy-preserving identity systems*. Inter-American Development Bank.
<https://publications.iadb.org/en/lacchain-id-framework-set-recommendations-blockchain-based-interoperable-privacy-preserving>
- Arias, F. G. (2012). *El proyecto de investigación: Introducción a la metodología científica* (6.^a ed.). Editorial Episteme.
<https://books.google.com.co/books?hl=es&id=W5n0BgAAQBAJ&printsec=frontcover>
- Auditoría General de la Nación. (2022). *Informe anual de auditorías 2021*.
<https://www.agn.gov.ar/informes>
- Banco Mundial. (2022). *GovTech Maturity Index: 2022 update—Trends in public sector digital transformation*.
<https://documents1.worldbank.org/curated/en/099035001132365997/pdf/P1694820bcef0903e091160315d2050d03b.pdf>
- Banco de la República. (2023, 29 de agosto). *Banco de la República, la Superintendencia Financiera de Colombia, IDB Invest y Davivienda realizaron pruebas para emisión y negociación de un bono digital*. <https://www.banrep.gov.co/es/noticias/banco-republica-superintendencia-financiera-colombia-idb-invest-davivienda-realizaron-pruebas>
- Banco Interamericano de Desarrollo. (2020). *Blockchain: Un modelo para el gobierno abierto en América Latina y el Caribe*. <https://publications.iadb.org/en/blockchain-model-open-government-latin-america-and-caribbean>

- Barker, E. (2020). *Recommendation for key management: Part 1—General (SP 800-57, Part 1, Rev. 5)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-57pt1r5>
- BID Invest. (2023, 3 de marzo). *IDB Invest completes first tradable bond tokenization in Latin America and the Caribbean*. <https://idbinvest.org/es/medios-y-prensa/bid-invest-lanza-una-historica-titulizacion-de-us1000-millones-en-america-latina-y-el>
- Blockchain Federal Argentina. (s. f.). *Acerca de BFA*. <https://bfa.ar/>
- Brown, S. (s. f.). *The C4 model for visualising software architecture*. <https://c4model.com/>
- Bunge, M. (2004). *La ciencia, su método y su filosofía*. Debolsillo. https://books.google.com/books?id=_YtMPgAACAAJ
- Cambo Chillo, L. V. (2022). *Análisis comparativo del sistema de auditoría tradicional y un sistema de auditoría Blockchain e IPFS*. <https://dspace.utb.edu.ec/handle/49000/11589>
- Chen, P. P.-S. (1976). The entity-relationship model—Toward a unified view of data. *ACM Transactions on Database Systems*, 1(1), 9–36. <https://bit.csc.lsu.edu/~chen/pdf/erd-5-pages.pdf>
- Chile. (1999). *Ley N° 19.628 sobre protección de la vida privada*. Biblioteca del Congreso Nacional de Chile. <https://www.bcn.cl/leychile/navegar?idNorma=141599>
- Chile. (2008). *Ley N° 20.285 sobre acceso a la información pública*. Biblioteca del Congreso Nacional de Chile. <https://www.bcn.cl/leychile/navegar?idNorma=276363>
- Comisión Nacional de Energía. (2018a, febrero 27). *Comisión Nacional de Energía se convertirá en la primera entidad pública en utilizar Blockchain en Chile*. <https://www.cne.cl/prensa/prensa-2018/02-febrero-2018/comision-nacional-de-energia-se-convertira-en-la-primera-entidad-publica-en-utilizar-blockchain-en-chile/>
- Comisión Nacional de Energía. (2018b, abril 5). *Ministra Jiménez lanza tecnología Blockchain en datos del sector energético*. <https://www.cne.cl/prensa/prensa-2018/04-abril-2018/ministra-jimenez-lanza-tecnologia-blockchain-en-datos-del-sector-energetico/>
- Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Marco integrado de control interno: Marco y anexos* (versión en español). COSO. https://www.oas.org/juridico/pdfs/mesicic5_mex_ane_101.pdf
- Committee of Sponsoring Organizations of the Treadway Commission. (2020). *Blockchain and internal control: The COSO perspective*. https://www.coso.org/_files/ugd/3059fc_20098cf01dfe4bacb2cc2d289b15ebfb.pdf
- Cortés, F. J., & Torres, H. (2022). *La interdisciplinariedad de la profesión contable y el blockchain: Una breve revisión de sus implicaciones*. *Revista En-contexto*, 10(15), 115–134. <https://ojs.tdea.edu.co/index.php/encontexto/article/view/1445>

- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE. <https://study.sagepub.com/creswell3e>
- Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3), 5–21. <https://doi.org/10.2308/isis-51804>
- Decreto 102/1999. (1999). *Créase la Oficina Anticorrupción en el ámbito del Ministerio de Justicia y Derechos Humanos*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=61724>
- Decreto 117/2016. (2016). *Plan de Apertura de Datos*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=257755>
- Decreto 1023/2001. (2001). *Régimen de Contrataciones de la Administración Nacional*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/72179/norma.htm>
- Decreto 1030/2016. (2016). *Reglamento del Régimen de Contrataciones de la Administración Nacional*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=265506>
- Decreto 561/2016. (2016). *Sistema de Gestión Documental Electrónica (GDE)*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/307033/norma.htm>
- Decreto 780/2024. (2024). *Derecho de Acceso a la Información Pública. Reglamentación de la Ley 27.275. Modificación del Decreto 206/2017*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=403572>
- Decreto 1063/2016. (2016). *Plataforma de Trámites a Distancia (TAD)*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=266197>
- Decreto 1179/2016. (2016). *Reglamentación del artículo 18 de la Ley 25.188 (Registro de obsequios y viajes financiados por terceros)*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268471/norma.htm>
- Decreto 277/2018. (2018). *Reglamentación de la Ley 27.401 de Responsabilidad Penal de las Personas Jurídicas*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/308488/norma.htm>
- Decreto 182/2019. (2019). *Reglamentación de la Ley 25.506 de Firma Digital*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=322333>
- European Data Protection Board (EDPB). (2025). *Guidelines 02/2025 on processing of personal data through blockchain technologies* (Public consultation). EDPB. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en
- European Union Agency for Cybersecurity (ENISA). (2017). *Distributed Ledger Technology & Cybersecurity—Improving information security in the financial sector*. ENISA. <https://www.enisa.europa.eu/publications/blockchain-security/>

- e-Estonia. (2021). *How Estonia uses blockchain technology*. <https://e-estonia.com/solutions/security-and-safety/blockchain/>
- Foro Económico Mundial & Banco Interamericano de Desarrollo. (2020). *La cadena de bloques para contrataciones públicas en América Latina y el Caribe*. World Economic Forum. <https://www.weforum.org/whitepapers/blockchain-for-public-procurement-in-latin-america/>
- Gestión. (2020, 3 de septiembre). *Perú Compras registra más de 154,000 órdenes de compra en blockchain*. <https://gestion.pe/economia/peru-compras-registra-mas-de-154000-ordenes-de-compra-en-blockchain-noticia/>
- Gobierno de la Ciudad de Buenos Aires. (2023, 9 de octubre). *Identidad digital autosoberana: QuarkID*. <https://www.buenosaires.gob.ar/innovacion/quarkid>
- Gobierno de la Ciudad de Buenos Aires. (2024). *Resolución N.º 758991 (PDF)*. <https://boletinoficial.buenosaires.gob.ar/normativaba/norma/pdf/758991>
- Gobierno de la Ciudad de Buenos Aires. (2025, 7 de mayo). *Certificados de Salud en miBA*. <https://buenosaires.gob.ar/noticias/certificados-de-salud-en-miba>
- Gobierno de la Ciudad de Buenos Aires. (s. f.). *¿Qué es QuarkID?* <https://buenosaires.gob.ar/desarrollo-urbano/quarkid>
- González González, C. A. (2023). *El blockchain en las finanzas públicas y su uso para el combate a la corrupción* (Tesis de maestría, Universidad Nacional Autónoma de México). <https://ru.dgb.unam.mx/server/api/core/bitstreams/e5e14feb-2b04-4e4e-b76a-1775e2b1d500/content>
- Grigg, I. (2005). *Triple entry accounting*. https://iang.org/papers/triple_entry.html
- Grupo de los Veinte (G20). (2024). *G20 Anti-Corruption Working Group Accountability Report 2024*. G20. https://track.unodc.org/uploads/documents/corruption/G20-Anti-Corruption-Resources/Accountability-and-Monitoring-Reports/2024_G20_Brazil_ACWG_Accountability_Report_2024_-_Organizing_against_corruption.pdf
- Hiatt, J. M. (2006). *ADKAR: A model for change in business, government and our community*. Prosci. https://books.google.com/books?id=Te_cHbWv-ZgC
- Hernández, R., Fernández, C., & Baptista, P. (2022). *Metodología de la investigación* (7.ª ed.). McGraw-Hill. https://www.uv.mx/personal/cbustamante/files/2011/06/metodologia-de-la-investigaci%C3%83%C2%B3n_sampieri.pdf
- International Organization for Standardization (ISO). (2018). *ISO 19011:2018—Guidelines for auditing management systems*. ISO. <https://www.iso.org/standard/70017.html>

- International Organization for Standardization (ISO). (2019). *ISO 8601-1:2019—Date and time—Representations for information interchange—Part 1: Basic rules*. ISO. <https://www.iso.org/standard/70907.html>
- International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2013). *ISO/IEC 19510:2013—Information technology—Business Process Model and Notation (BPMN)*. ISO. <https://www.iso.org/standard/62652.html>
- International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2015). *ISO/IEC 27041:2015—Guidance on assuring suitability and adequacy of incident investigative method*. ISO. <https://www.iso.org/standard/44405.html>
- International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2015). *ISO/IEC 27043:2015—Incident investigation principles and processes*. ISO. <https://www.iso.org/standard/44407.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2012). *ISO/IEC 27037:2012—Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO. <https://www.iso.org/standard/44381.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *ISO/IEC 27001:2022—Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO. <https://www.iso.org/standard/27001.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *ISO/IEC 27002:2022—Information security, cybersecurity and privacy protection—Information security controls*. ISO. <https://www.iso.org/standard/75652.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *ISO/IEC 27005:2022—Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. ISO. <https://www.iso.org/standard/80585.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2023). *ISO/IEC 27035-1:2023—Information technology—Information security incident management—Part 1: Principles and process*. ISO. <https://www.iso.org/standard/78973.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2008). *ISO/IEC 25012:2008—Software engineering—Software product Quality Requirements and Evaluation (SQuaRE)—Data quality model*. ISO. <https://www.iso.org/standard/35736.html>
- International Organization for Standardization (ISO). (2018). *ISO 31000:2018—Risk management—Guidelines*. ISO. <https://www.iso.org/standard/65694.html>

- International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2019). *ISO/IEC 31010:2019—Risk management—Risk assessment techniques*. ISO. <https://www.iso.org/standard/72140.html>
- International Organization for Standardization (ISO). (2021). *ISO 37301:2021—Compliance management systems—Requirements with guidance for use*. ISO. <https://www.iso.org/standard/75080.html>
- International Organization for Standardization (ISO). (2025). *ISO 37001:2025—Anti-bribery management systems—Requirements with guidance for use*. ISO. <https://www.iso.org/standard/37001>
- International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), & Institute of Electrical and Electronics Engineers (IEEE). (2011). *ISO/IEC/IEEE 42010:2011—Systems and software engineering—Architecture description*. ISO/IEEE. <https://www.iso.org/standard/50508.html>
- International Organization for Standardization (ISO). (2019). *ISO 22301:2019—Security and resilience—Business continuity management systems—Requirements*. ISO. <https://www.iso.org/standard/75106.html>
- International Organization for Standardization (ISO). (2018). *ISO 50001:2018—Energy management systems—Requirements with guidance for use*. ISO. <https://www.iso.org/standard/69426.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2016). *ISO/IEC 30134-2:2016—Information technology—Data centre facilities and infrastructures—Key performance indicators—Part 2: Power Usage Effectiveness (PUE)*. ISO. <https://www.iso.org/standard/63451.html>
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2016). *ISO/IEC 30134-3:2016—Information technology—Data centre facilities and infrastructures—Key performance indicators—Part 3: Renewable Energy Factor (REF)*. ISO. <https://www.iso.org/standard/66127.html>
- International Organization of Supreme Audit Institutions (INTOSAI). (2013). *ISSAI 100—Fundamental principles of public-sector auditing*. INTOSAI. <https://www.issai.org/>
- Inter-American Development Bank. (2022, 23 de agosto). *Inter-American Development Bank and Davivienda successfully carry out a pilot to register the first blockchain-based bond in Colombia*. <https://www.iadb.org/en/news/idb-group-and-davivienda-bank-issue-colombias-first-blockchain-bond>
- Inter-American Development Bank. (2018, 3 de agosto). *The Bahamas pioneers Blockcerts for development*. <https://blogs.iadb.org/caribbean-dev-trends/en/the-bahamas-pioneers-blockcerts-for-development/>

- Kaleido. (2019, 19 de diciembre). *Announcing GA and production support for Hyperledger Besu: IBFT 2.0 has immediate finality*. <https://www.kaleido.io/blockchain-blog/hyperledger-besu-protocol-for-enterprise-ethereum-blockchain>
- Kaleido. (2023, 1 de septiembre). *Consensus algorithms compared: PoA vs IBFT vs Raft*. <https://www.kaleido.io/blockchain-blog/consensus-algorithms-poa-ibft-or-raft>
- Kotter, J. P. (2012). *Leading change*. Harvard Business Review Press. <https://store.hbr.org/product/leading-change-with-a-new-preface-by-the-author/11116>
- LACChain Identity Working Group. (2021). *LACChain ID Framework: Recommendations for interoperable, privacy-preserving and regulatory-compliant digital identifiers, credentials and wallets*. Inter-American Development Bank. <https://publications.iadb.org/publications/english/document/LACChain-ID-Framework-A-Set-of-Recommendations-for-Blockchain-Based-Interoperable-Privacy-Preserving-Regulatory-Compliant-Secure-and-Standardized-Digital-Identifiers-Credentials-and-Wallets.pdf>
- Ley 24.156. (1992). *Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/554/texact.htm>
- Ley 27.275. (2016). *Ley de Derecho de Acceso a la Información Pública*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>
- Ley 25.188. (1999). *Ley de Ética en el Ejercicio de la Función Pública*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=60897>
- Ley 25.326. (2000). *Ley de Protección de Datos Personales*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>
- Ley 25.506. (2001). *Régimen legal de la firma digital*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm>
- Ley 27.401. (2017). *Responsabilidad Penal de las Personas Jurídicas*. Infoleg. <https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=296846>
- Luna González Becerril, M. L. (2020). *La tecnología blockchain y su impacto en el sector público en México. Análisis del caso Blockchain HACKMX* (Tesis de maestría, Universidad Nacional Autónoma de México). <https://ru.dgb.unam.mx/server/api/core/bitstreams/472dc843-b6f4-49ca-afdf-9616355be211/content>
- Ministerio de Servicio Público de Bahamas. (2018, 15 de febrero). *LTA selects Blockcerts and Learning Machine to issue workforce certificates*. <https://www.bahamas.gov.bs/wps/portal/public/gov/government/news/lta+selects+blockcerts+and+learning+machine+to+issue+workforce+certificates>

- Morales, D. (2021). *Impacto del blockchain en la contabilidad y auditoría*. Revista Conrado, 17(80), 142–150. <https://www.redalyc.org/articulo.oa?id=759781282017>
- National Institute of Standards and Technology (NIST). (2019). *FIPS PUB 140-3: Security requirements for cryptographic modules*. NIST. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>
- National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). NIST. <https://www.nist.gov/cyberframework>
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
- Oficina Anticorrupción (OA). (s. f.). *Portal institucional de la Oficina Anticorrupción*. Argentina.gob.ar. <https://www.argentina.gob.ar/justicia/anticorrupcion>
- Oficina Anticorrupción (OA). (2025, 17 de junio). *La OA prorrogó la presentación de DDJJ 2024 hasta el 31 de julio*. Argentina.gob.ar. <https://www.argentina.gob.ar/justicia/anticorrupcion/noticias/la-oa-prorrogo-la-presentacion-de-ddjj-2024-hasta-el-31-de-julio>
- Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD). (2004). *Convención de las Naciones Unidas contra la Corrupción*. ONU. <https://www.unodc.org/unodc/en/corruption/convention.html>
- Open Government Partnership. (2019). *Assessing OGP values for relevance*. <https://www.opengovpartnership.org/wp-content/uploads/2019/06/OGPvaluesguidancenote.pdf>
- Organización de las Naciones Unidas (ONU). (2015). *Transformar nuestro mundo: La Agenda 2030 para el Desarrollo Sostenible (Resolución A/RES/70/1)*. ONU. <https://sdgs.un.org/es/2030agenda>
- Organización de los Estados Americanos (OEA). (1996). *Convención Interamericana contra la Corrupción*. OEA. https://www.oas.org/es/sla/dil/tratados_B-58_convencion_interamericana_contra_la_corrupcion.asp
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2014). *Recommendation of the Council on digital government strategies*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406>
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2017). *Recommendation of the Council on public integrity*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0435>
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2020). *The OECD digital government policy framework: Six dimensions of a digital government* (OECD Public Governance Policy Papers, No. 02). https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/the-oecd-digital-government-policy-framework_11dd6aa8/f64fed2a-en.pdf

- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2020). *Manual de la OCDE sobre integridad pública*. OCDE.
https://www.oecd.org/content/dam/oecd/es/publications/reports/2020/05/oecd-public-integrity-handbook_598692a5/8a2fac21-es.pdf
- Perú Compras – Central de Compras Públicas. (2020, 2 de septiembre). *Perú Compras registró en blockchain más de 154 mil órdenes de compra*.
<https://www.gob.pe/institucion/perucompras/noticias/297606-peru-compras-registro-en-blockchain-mas-de-154-mil-ordenes-de-compra>
- Perú Compras – Central de Compras Públicas. (2021, 9 de julio). *Resolución Jefatural N.º 139-2021-Perú Compras: Aprueban la Directiva N.º 006-2021-Perú Compras*.
<https://www.gob.pe/institucion/perucompras/normas-legales/2017772-139-2021-peru-compras>
- Polimandi, D. M. (2023). *El contador y auditor frente a la nueva tecnología blockchain como participante clave en la fiabilidad de la información contable* (Trabajo final de posgrado, Universidad de Buenos Aires). http://bibliotecadigital.econ.uba.ar/download/tpos/1502-3047_PolimandiD.pdf
- Project Management Institute (PMI). (2021). *A guide to the project management body of knowledge (PMBOK® Guide)* (7.ª ed.). PMI. <https://www.pmi.org/pmbok-guide-standards/foundational/pmbok>
- QuarkID. (s. f.). *What is QuarkID*. <https://www.quarkid.org/>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (SP 800-207)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
- Sabino, C. (2014). *El proceso de investigación*. Editorial Episteme.
https://books.google.com/books/about/El_proceso_de_investigaci%C3%B3n.html?id=jwejBAAQBAJ
- Santos, M. C. (2022). *Blockchain y su implicancia en la contabilidad*. Universidad Nacional de La Plata.
<https://www.econo.unlp.edu.ar/frontend/media/91/31591/698cda75dc3c598f564400184518de2e.pdf>
- Schmitz, J., & Leoni, G. (2019). *Accounting and auditing at the time of blockchain technology*. *Australian Accounting Review*, 29(2), 331–342. <https://doi.org/10.1111/auar.12286>
- Szabo, N. (1997). *Formalizing and Securing Relationships on Public Networks*. *First Monday*.
<https://firstmonday.org/ojs/index.php/fm/article/view/548>
- Superintendencia Financiera de Colombia. (2022, 9 de agosto). *Prueba piloto de emisión de bono en blockchain*. <https://www.superfinanciera.gov.co/publicaciones/10111998/sala-de-prensacomunicados-de-prensa-comunicados-de-prensa-culmina-con-exito-prueba-piloto-de>

emision-de-un-bono-usando-tecnologia-blockchain-en-la-renera-de-la-superintendencia-financiera-10111998/

- Tashakkori, A., & Teddlie, C. (Eds.). (2010). *SAGE handbook of mixed methods in social & behavioral research* (2nd ed.). SAGE. <https://us.sagepub.com/en-us/nam/sage-handbook-of-mixed-methods-in-social-behavioral-research/book233405>
- Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger (Yellow Paper)*. <https://ethereum.github.io/yellowpaper/paper.pdf>
- World Wide Web Consortium (W3C). (2017, 31 de enero). *Data on the Web Best Practices* (W3C Recommendation). W3C. <https://www.w3.org/TR/dwbp/>
- Yazuma Carrillo, J. A. (2023). *Escenario prospectivo para el desarrollo de blockchain en la contratación pública del Ecuador al 2030* (Tesis de maestría, Instituto de Altos Estudios Nacionales). <https://repositorio.iaen.edu.ec/jspui/handle/24000/6355>