

Soberanía digital:

Breve estado del arte global y latinoamericano

DOI: 10.29236/sistemas.n180a4

Jeimy J. Cano M.

Resumen

Este artículo ofrece un estado del arte sobre la soberanía digital, desde sus raíces conceptuales hasta la disputa actual por la inteligencia artificial, con foco en América Latina y el Caribe. Se aplicó una revisión documental estructurada según PRISMA 2020 en versión simplificada, con síntesis narrativa de una base verificada de fuentes académicas e institucionales. Los hallazgos muestran que la soberanía digital funciona más como una práctica discursiva que como una categoría jurídica cerrada, que las grandes potencias siguen modelos distintos y que la región llega tarde y con dependencia estructural al debate. La inteligencia artificial agudiza esa brecha. Las conclusiones son provisionales por la velocidad del cambio tecnológico y el rezago regional, y se proponen caminos concretos de cooperación, gobernanza de datos e interdependencia gestionada para la ciberseguridad y ciberdefensa de América Latina y el Caribe.

Palabras clave

Soberanía digital, gobernanza de datos, inteligencia artificial, América Latina y el Caribe, ciberdefensa.

Introducción

La soberanía digital pasó de ser un término de nicho a ocupar el centro de la política tecnológica y de la ciberdefensa. Gobiernos y empresas la invocan para justificar decisiones sobre datos, redes, nube e inteligencia artificial. El problema es que el término significa cosas distintas según quién lo use. Pohle y Thiel (2020) muestran que se ha convertido en un concepto de uso común y a la vez muy disputado, presente tanto en democracias liberales como en regímenes centralizados.

Esa ambigüedad es un tema relevante. Fratini et al. (2024), tras revisar 271 artículos, concluyen que las distintas versiones del concepto comparten un núcleo común, la idea de control sobre datos e infraestructura, pero divergen en quién ejerce ese control y con qué fin. Cuando un mismo término sirve para proteger derechos o para restringirlos, conviene precisar de qué se habla antes de recomendar o diseñar políticas.

Este trabajo tiene como objetivo hacer una revisión conceptual de la soberanía digital y ubicar en él a América Latina y el Caribe. La revisión se organiza en cuatro ejes. Primero, la genealogía del concepto. Segundo, los modelos que adoptan las principales potencias digitales. Tercero, la situación regional. Cuarto, el papel de la inteligencia artificial como nuevo terreno de tensiones. El enfoque es el de la

ciberseguridad y la ciberdefensa, es decir, se pregunta no solo qué significa el concepto, sino qué implica para quien debe proteger activos digitales y tomar las decisiones críticas.

Método

La revisión se realizó siguiendo la declaración PRISMA 2020 (Page et al., 2021) en una versión simplificada. Se conserva el esqueleto de reporte de PRISMA, criterios de elegibilidad, fuentes de información, proceso de selección, extracción y síntesis. Se declara de forma transparente que el método PRISMA 2020 fue diseñado para revisiones de intervenciones en salud, por lo que su uso aquí es una adaptación, no un ajuste literal. En este sentido, se aplica una valoración por tipo de fuente, distinguiendo literatura arbitrada, informes de organismos internacionales y literatura gris de consultoras o centros de pensamiento.

Los criterios de elegibilidad fueron: pertinencia temática con la soberanía digital, idioma español o inglés, y ventana temporal de 2020 a 2024 para las fuentes complementarias, con extensión a 2026 solo en el eje de inteligencia artificial, donde la evidencia reciente es clave. Las fuentes complementarias se identificaron mediante búsquedas en la web y se verificaron cada una de ellas. La síntesis es narrativa y temática, organizada según los cuatro ejes.

Un breve resumen del proceso se presenta a continuación:

- Identificación
 - Búsquedas en la web con las siguientes cadenas: “digital sovereignty systematic review 2020..2024 concept”, “soberanía digital América Latina 2020..2024 revista académica”, “AI sovereignty” OR “sovereign AI” governance compute 2023 2024 peer reviewed, “digital sovereignty Caribbean CEPAL data governance Latin America 2022 2023 2024”
 - Registros recuperados en búsquedas web académicas: ~55
 - Artículos base iniciales: 6
- Filtrado
 - Registros web tras quitar duplicados: ~40
 - Excluidos por duplicación (mismo trabajo en varios repositorios): ~15
- Registros pertinentes al tema: ~25
 - Excluidos por no pertinencia: ~15 (detectores de texto de IA, herramientas, notas de prensa, páginas de listado)
- Elegibilidad - Evaluados por texto o resumen: ~18
 - Excluidos por estar fuera de la ventana temporal o no ser verificables: ~7
- Complementarias incluidas: 10

- Excluidos por redundancia o carácter secundario: ~9 (literatura gris del eje de IA ya cubierta por otras fuentes)

- Incluidas en la síntesis
 - 10 fuentes complementarias verificadas, 6 referencias base (5 temáticas y 1 guía metodológica) + dos referencias relevantes a notas en internet = 18 en total

Nota: La cifra de ~55 registros es aproximada, por sumar resultados de varias búsquedas antes de depurar; los números intermedios son una reconstrucción del ejercicio de filtrado, no un conteo auditado paso a paso. El resultado final: 10 fuentes complementarias incluidas, 6 básicas y dos referencias a notas en internet. 18 en total.

Resultados

Genealogía del concepto

La soberanía es no es una idea reciente. En el siglo XVI, Bodin la asoció a la autoridad última del gobernante; más tarde, Rousseau la desplazó hacia la soberanía popular, y con el tiempo quedó ligada a la democracia, el Estado de derecho y el territorio (Pohle & Thiel, 2020). En su forma moderna, la soberanía combina independencia frente a otros Estados y poder supremo dentro del propio territorio.

Con la llegada de internet, muchos creyeron que el Estado perdería relevancia. La Declaración de Inde-

pendencia del Ciberespacio de Barlow (1996) expresó esa ilusión: un espacio virtual ajeno al control gubernamental. Pohle y Thiel (2020) llaman a esa corriente excepcionalismo del ciberespacio. A ella se sumó, desde el año 2000, la gobernanza multiactor, que proponía administrar internet mediante la colaboración de los directamente afectados y no de los Estados. Ninguna de las dos cumplió su promesa. La comercialización de internet y la aparición de plataformas dominantes facilitaron, más bien, la observación y el control de los flujos digitales.

El giro decisivo llegó con dos hechos. Primero, la constatación de que el poder que desafía al Estado no está en la red como un todo (internet), sino en corporaciones que controlan infraestructuras vitales y actúan como actores casi soberanos. Segundo, las revelaciones de Snowden en 2013 sobre vigilancia masiva, que dispararon la demanda de control nacional sobre datos y comunicaciones (Pohle & Thiel, 2020). Fratini et al. (2024) sitúan justamente en 2014, el año posterior a esas revelaciones, el punto de arranque de la difusión del concepto.

Couture y Toupin (2019) aportan una advertencia relevante al sostener que la soberanía funciona como un "acto de habla": aparece con fuerza allí donde la autoridad es débil o disputada, mientras que está casi ausente en los Estados

Unidos, nación que concentra gran parte del poder de internet. Esta lectura, que entiende la soberanía digital como un discurso antes que como una norma, es hoy la más sólida y guía la presente reflexión.

En esa misma línea, Pohle (2024) invita a "repensar" este concepto y advierte que, debido a su uso constante para fines opuestos, el término corre el riesgo de volverse impreciso y de servir para justificar casi cualquier decisión política o medida regulatoria.

En este sentido, a nivel regional, el discurso de la soberanía tecnológica se erige como un pilar estratégico de estabilidad política, en el cual el control local de la infraestructura crítica y los datos sensibles se vuelve indispensable para asegurar la supervivencia y resiliencia estatal frente a la asimetría de las amenazas externas (Rubio Piñeiro, 2024).

Actores y niveles de reclamo

Quien reclama soberanía digital no siempre es un Estado. Pohle y Thiel (2020) distinguen tres capas de reclamos: la autonomía y seguridad de las infraestructuras nacionales, la autonomía de la economía frente a proveedores extranjeros, y la autodeterminación del individuo como usuario y ciudadano. Couture y Toupin (2019) amplían el mapa con cinco perspectivas, que suman a los Estados los pueblos indígenas, los movimientos sociales y la persona, además de la vieja idea de un ciberespacio autogobernado.

Esa pluralidad importa para la región. En América Latina, colectivos sociales construyen soberanía digital desde abajo, con software libre, servidores propios y prácticas de resistencia frente al internet corporativo, en una línea que enlaza con la soberanía alimentaria y con la crítica al colonialismo digital (Guerra-González et al., 2022). El concepto, por tanto, no pertenece solo a los ministerios; también es una bandera de la sociedad civil.

Modelos de las principales potencias digitales

Las grandes potencias no persiguen la misma soberanía. Fratini et al. (2024) proponen cuatro modelos según cómo y por qué se busca el control: uno basado en derechos, uno orientado al mercado, uno de centralización y uno centrado en el Estado. China fue pionera al reivindicar el control soberano del ciberespacio; la Unión Europea llegó después, apoyándose en la regulación y en la defensa de derechos fundamentales.

El caso europeo es el más citado. Gaia-X, lanzado en 2020, busca una infraestructura de datos federada y conforme a estándares europeos, como alternativa a los grandes proveedores de nube extranjeros (Deloitte, 2025; Pohle & Thiel, 2020). Estados Unidos ofrece el contraste: su ventaja está en las empresas que dominan la nube y los modelos de inteligencia artificial, y su marco legal, con la CLOUD Act de 2018, permite el

acceso a datos incluso alojados fuera del país bajo ciertas circunstancias (Arthur D. Little, 2026). Rusia desarrolló una internet soberana que puede aislarse en caso de amenaza, y los países BRICS coordinan esfuerzos para reducir su dependencia de plataformas occidentales (Deloitte, 2025).

Para pasar del discurso a la práctica, Arthur D. Little (2026) propone mirar tres soberanías: la de los datos, referida a dónde residen y qué leyes los gobiernan; la de los sistemas, sobre el control de la infraestructura; y la de la decisión, la capacidad de elegir y sostener las propias decisiones tecnológicas cuando cambian las condiciones. La soberanía, en esta lectura, no es algo que activa o desactiva, sino un conjunto de elecciones deliberadas a lo largo de la cadena tecnológica.

América Latina y el Caribe

La región por lo general resulta alejada de estos debates y más en una postura dependiente. Becerra y Waisbord (2024) documentan la llamativa ausencia de América Latina en el debate mundial sobre soberanía digital y describen dos décadas de un enfoque desregulador que dejó a las plataformas globales operar con pocos límites. El dato institucional acompaña esa lectura: en el índice de gobierno digital para la región, el promedio regional queda muy por debajo del promedio de los países de la OCDE, con avances desiguales entre países (OECD & CAF, 2023).

Esta brecha deja de ser una abstracción regulatoria para convertirse en una vulnerabilidad de seguridad nacional. Por ejemplo, la proliferación de tecnologías extrarregionales vinculadas al Estado chino en la videovigilancia urbana de ciudades inteligentes facilita la recopilación de inteligencia extranjera directa. Un caso crítico de esta exposición geopolítica ocurrió en noviembre de 2024, cuando el grupo de espionaje de origen estatal Flax Typhoon logró infiltrar sistemáticamente la infraestructura de información del Gobierno paraguayo (CEEP, 2024).

Aun así, hay movimiento. La agenda digital regional coordinada por la CEPAL fija prioridades comunes de conectividad, capacidades e innovación, aunque el desarrollo entre países sigue siendo dispar (CEPAL, 2022). En el plano histórico, programas satelitales como el Sistema Morelos de México o el Vene-sat-1 venezolano de 2008 mostraron que el control de infraestructura orbital también hace parte de la autonomía tecnológica (Deloitte, 2025).

El Caribe merece una revisión especial. Sus pequeños Estados insulares son especialmente vulnerables a desastres naturales, fallos de conectividad y ciberataques. Frente a ello, la CEPAL (2025) estudió las embajadas de datos, arreglos de estatus diplomático que otorgan jurisdicción soberana sobre servidores alojados en el extranjero y

garantizan la continuidad del Estado ante una crisis, inspirados en el modelo de Estonia. Es un ejemplo concreto de soberanía de datos adaptada a una realidad regional. La evidencia arbitrada específica sobre el Caribe, sin embargo, es escasa, y se apoya sobre todo en informes de organismos internacionales.

La inteligencia artificial como nuevo campo de disputa soberana

La inteligencia artificial traslada la disputa a un terreno más exigente. Srivastava y Bullock (2024) muestran que Estados y empresas usan la IA para ampliar su poder en tres planos, el instrumental, el estructural y el discursivo, y que la soberanía se juega tanto en el control de las infraestructuras como en la competencia por desarrollarlas. Su tesis central es que la IA no reemplaza al Estado, sino que confunde aún más el poder público con el privado.

Arthur D. Little (2026) añade una alerta operativa. A medida que la IA deja de ser una herramienta de productividad y se convierte en una capa que planifica y coordina procesos, requisitos como la portabilidad, la auditabilidad y la capacidad de salida (*poder abandonar a un proveedor o tecnología y migrar a otro sin quedar atrapado, con rutas de salida diseñadas y probadas de antemano, no solo supuestas*) se vuelven más complejos y costosos de incorporar después. La firma

habla de “deuda de soberanía” para nombrar esas dependencias ocultas que luego cuesta deshacer.

Conviene, sin embargo, no confundir soberanía con autarquía (*forma extrema de autosuficiencia tecnológica que lleva al aislamiento digital, con desconexión de la red global y restricción del acceso a tecnologías externas* (Deloitte, 2025).). Tanner et al. (2026) sostienen que una soberanía de la IA de arquitectura completa es estructuralmente inviable para casi cualquier país, porque la cadena de la IA, desde los minerales y la energía hasta el cómputo y los modelos, cruza fronteras. Proponen una interdependencia gestionada: mapear dependencias por capa (*minerales, energía, chips (cómputo), redes, infraestructura, datos, modelos y aplicaciones, talento y la gobernanza*), diversificar proveedores y socios, y asegurar interoperabilidad mediante estándares y contratos. Este informe procede de un centro de pensamiento que declara como donantes a grandes empresas tecnológicas, dato que conviene tener presente al leer sus recomendaciones. Para América Latina y el Caribe, con capacidades de cómputo limitadas, la interdependencia gestionada parece más realista que la aspiración a una autonomía total.

Este realismo operativo se agudiza al evaluar el Digital Sovereignty Index de la región, el cual evidencia que América Latina y el Caribe mantiene una dependencia estructural

casi absoluta de hardware sofisticado, computación de alto rendimiento y nubes extranjeras para desarrollar su propia tecnología, lo que restringe el desarrollo autónomo de soluciones de IA soberanas (Yepes, 2026).

Dimensión organizacional

La soberanía digital también se decide dentro de las organizaciones. Follette et al. (2021) identifica cuatro maneras de gestionar el riesgo geopolítico, desde las empresas que lo tratan como fuente de oportunidad e integran su análisis en la estrategia, hasta las que solo reaccionan de forma defensiva y con procesos mínimos. La diferencia entre unas y otras no es el tamaño, sino la madurez de sus procesos y su disposición a anticiparse.

Ese enfoque conecta con la propuesta de Arthur D. Little (2026) de clasificar los activos por niveles según su criticidad y la viabilidad de reducir la dependencia. No todo requiere el mismo grado de control: algunos activos justifican inversiones estratégicas de largo plazo, mientras que otras dependencias pueden tolerarse como una decisión económica deliberada. Para la ciberseguridad y ciberdefensa regional, esta lógica de priorización es más útil que una consigna de soberanía aplicada a todo por igual.

Dicha priorización es imperativa hoy en día, ya que la línea que separaba la ciberseguridad corporativa del ciberconflicto geopolítico militar

se ha venido desvaneciendo. Al delegar flujos de información críticos a proveedores de nube hiperscalares expuestos a tensiones geopolíticas de sus países de origen, las organizaciones de la región pierden soberanía operativa sobre sus datos de monitoreo, inteligencia y capacidad de respuesta activa.

Discusión

Los resultados de esta revisión dejan tres tensiones de fondo. La primera opone *soberanía y aislamiento*. Tener soberanía digital no significa cerrar fronteras tecnológicas, sino definir las condiciones bajo las cuales se abren; cuando se prohíben servicios extranjeros sin alternativas viables, la soberanía se degrada en aislamiento (Deloitte, 2025). La segunda enfrenta *control y competitividad*: un enfoque rígido de soberanía primero puede encarecer, frenar la innovación y restar competitividad (Arthur D. Little, 2026). La tercera opone *seguridad y derechos*, pues las medidas que refuerzan el control estatal pueden, mal diseñadas, restringir la privacidad y la libertad de expresión en lugar de protegerlas (Pohle & Thiel, 2020).

Para la ciberseguridad y ciberdefensa de América Latina y el Caribe, la implicación es directa. La región combina alta dependencia tecnológica, marcos regulatorios desiguales y poca presencia y capacidad de influencia en los foros donde se fijan las reglas. Pohle y

Thiel (2020) advierten que la soberanía digital es un medio, no un fin. Quien la ejerce, sea un gobierno o una empresa, debe responder ante la ciudadanía por cómo la usa. Esto importa aún más donde las instituciones son débiles, porque allí el mismo poder que promete defensa puede terminar usándose para controlar o vigilar sin control.

Limitaciones

La base documental es acotada y la revisión sigue PRISMA en versión simplificada, por lo que no es exhaustiva. Varias fuentes provienen de consultoras y centros de pensamiento, con encuadres comerciales que se han señalado caso por caso. La evidencia arbitrada sobre el Caribe es escasa y se complementa con informes institucionales. Existe además un sesgo de idioma y de publicación, al privilegiar textos en español e inglés.

Por último, en el eje de inteligencia artificial buena parte de la evidencia de 2025 y 2026 es literatura de consultoras o centros de pensamiento, de modo que las conclusiones en ese punto son especialmente provisionales.

Conclusiones y recomendaciones

La soberanía digital se entiende mejor como una práctica discursiva y política que como una categoría jurídica cerrada (Couture & Toupin, 2019; Pohle & Thiel, 2020). Las potencias la ejercen con modelos distintos, desde el enfoque de dere-

chos europeo hasta el control estatal chino (Fratini et al., 2024). América Latina y el Caribe llega con retraso a esa conversación y con dependencia estructural (Becerra & Waisbord, 2024; OECD & CAF, 2023), y la inteligencia artificial amplía la brecha (Srivastava & Bullock, 2024; Tanner et al., 2026).

Estas conclusiones son provisionales. La evolución tecnológica es acelerada, sobre todo en inteligencia artificial, y el rezago de la región es evidente. Lo que hoy parece una recomendación sólida puede quedar desfasado en pocos años, por lo que este estado del arte debe leerse como una fotografía de un momento y no como una guía definitiva.

Con esta anotación, se proponen caminos concretos para la región. No son recetas, sino opciones fundadas en la evidencia revisada:

Cooperación regional. Actuar en bloque a través de la agenda digital coordinada por la CEPAL para superar la escala pequeña de los mercados nacionales (CEPAL, 2022).

- **Gobernanza de datos sensata.** Regular residencia y acceso a los datos sin caer en el aislamiento, distinguiendo soberanía de autarquía (Deloitte, 2025).
- **Interdependencia gestionada.** En inteligencia artificial, mapear dependencias, diversificar pro-

veedores y asegurar interoperabilidad, en lugar de perseguir una autonomía total inviable (Tanner et al., 2026).

- **Resiliencia para el Caribe.** Explorar mecanismos como las embajadas de datos para asegurar la continuidad del Estado en los pequeños Estados insulares (CEPAL, 2025).
- **Priorización por criticidad.** Concentrar los esfuerzos de soberanía donde el valor en riesgo es mayor, clasificando los activos por niveles (Arthur D. Little, 2026).
- **Talento e infraestructura local.** Invertir en formación y en infraestructura propia como base de la autonomía, tanto en el sector público como en el privado (Deloitte, 2025).
- **Enfoque de derechos y participación.** Fundar las políticas en los derechos digitales y participar activamente en los foros de gobernanza de la IA para evitar nuevas formas de dependencia (Fratini et al., 2024; Guerra-González et al., 2022).

Referencias

Arthur D. Little. (2026). *The trade-offs of digital sovereignty: A practical framework for implementing the right strategy*. Arthur D. Little.
<https://capital-riesgo.es/es/articles/the-trade-offs-of-digital-sovereignty-a-practical-framework-for-implementing-the-right-strategy/>

- Barlow, J. (1996). A Declaration of the Independence of Cyberspace. <https://www.eff.org/cyberspace-independence>
- Becerra, M., & Waisbord, S. (2024). Soberanía y nacionalismo en entornos digitales: la llamativa ausencia de América Latina en el debate mundial. *Signo y Pensamiento*, 43. <https://revistas.javeriana.edu.co/index.php/signoypensamiento>
- Follette, C., Gilbert, M., Haris, I., McAdoo, M., & Seshadri, P. (2021). *Turning geopolitical risk into strategic advantage*. BCG. <https://www.bcg.com/publications/2021/advantages-of-geopolitical-risk-management-organizations-and-processes>
- Centro de Estudios Estratégicos del Ejército del Perú - CEEEP (2024). <https://dialogo-americas.com/es/articulos/soberania-digital-en-latinoamerica-desafios-de-vigilancia-geopolitica-y-riesgo-del-crimen-organizado/>
- Comisión Económica para América Latina y el Caribe. (2022). *Una senda digital para el desarrollo sostenible de América Latina y el Caribe*. CEPAL. <https://repositorio.cepal.org/handle/11362/48461>
- Comisión Económica para América Latina y el Caribe. (2025). *Data embassies: An innovative approach to strengthening digital resilience in the Caribbean* (LC/TS.2025/99). CEPAL. <https://hdl.handle.net/11362/84445>
- Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Deloitte. (2025). *Soberanía digital como estrategia nacional: un enfoque holístico*. Deloitte. <https://www.deloitte.com/latam/es/industries/tmt/perspectives/soberania-digital-como-estrategia-nacional.html>
- Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*, 3(3). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4816020
- Guerra-González, J. T., Suárez-Estrada, M., & Cerratto-Pargman, T. (2022). Construyendo soberanía digital en América Latina: un análisis de las iniciativas de cuatro colectivos sociales. *Chasqui. Revista Latinoamericana de Comunicación*, (149), 227–242. <https://doi.org/10.16921/chasqui.v1i14.9.4628>
- Organisation for Economic Co-operation and Development, & CAF. (2023). *Digital government review of Latin America and the Caribbean: Building inclusive and responsive public services*. OECD Publishing. <https://doi.org/10.1787/29f32e64-en>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología*, 74(9), 790–799. <https://doi.org/10.1016/j.recesp.2021.06.016>
- Pohle, J. (2024). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*. <https://doi.org/10.1002/poi3.437>

- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
- Rubio Piñeiro, G. J. (2024). Soberanía Tecnológica - Ciberseguridad. *DERROTERO*, 18(02), 1–13. <https://doi.org/10.70554/Derrotero2024.v18n02.03>
- Srivastava, S., & Bullock, J. (2024). *AI, global governance, and digital sovereignty* [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2410.17481>
- Tanner, B., Kerry, C. F., Wyckoff, A. W., Kyosovska, N., Renda, A., & Tabassi, E. (2026). Is AI sovereignty possible? Balancing autonomy and interdependence. *Brookings Institution y CEPS*. <https://www.brookings.edu/articles/is-ai-sovereignty-possible-balancing-autonomy-and-interdependence/>
- Yepes, L. (2026). La inteligencia artificial avanza en América Latina, pero la región enfrenta un nuevo desafío: la soberanía digital. *Infobae*. <https://www.infobae.com/america/inhouse/2026/08/03/la-inteligencia-artificial-avanza-en-america-latina-pero-la-region-enfrenta-un-nuevo-desafio-la-soberania-digital/> 

Jeimy J. Cano M., Ph.D, Ed.D., CFE, CICA. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas–ACIS–.