

Edición
15

ISSN: 2953-769X

CIBERCONTABILIDAD



REVISTA SEMESTRAL



Universidad San Marcos
Revista Académica Institucional





PERSPECTIVA

Esta sección incluye artículos de opinión los cuales son caracterizados por presentar la postura, valoraciones y análisis sobre determinado asunto o acontecimiento de interés del autor.

LA CIBERCONTABILIDAD EN LA ERA DIGITAL: PERSPECTIVAS ÉTICAS, TÉCNICAS Y DE SEGURIDAD DE LA INFORMACIÓN EN COSTA RICA Y LATINOAMÉRICA

MAEd. Alejandro José Rodríguez Arguedas, alrodriguez@usam.ac.cr
Universidad San Marcos, San José, Costa Rica
Código ORCID <https://orcid.org/0009-0000-9470-9827>

DOI: <https://doi.org/10.64183/3k95b916>

Recibido: 16 de marzo de 2026

Aceptado: 22 de mayo de 2026

Resumen. La cibercontabilidad se ha convertido en un concepto emergente que integrada la contabilidad tradicional con tecnologías digitales y la ciberseguridad. Este artículo explora, desde una perspectiva académica, las implicaciones éticas, técnicas y de seguridad de la información asociadas a la transformación digital de la contaduría. Por lo tanto, en la práctica profesional empresarial como en la docencia universitaria. Mediante una metodología mixta (cuantitativa y cualitativa), se analiza el estado del arte global y regional, incorporando un estudio de caso aplicado en Costa Rica. Los hallazgos evidencian que la rápida digitalización contable plantea dilemas éticos (como la confidencialidad de datos y la transparencia algorítmica), desafíos técnicos (adopción de contabilidad 4.0, Inteligencia artificial, blockchain, computación en la nube) y riesgos significativos de ciberseguridad en la protección de la información financiera. En el contexto costarricense y latinoamericano, se observa una brecha entre la evolución tecnológica y los marcos normativos que se encuentran vigentes, así como una necesidad de fortalecer la formación profesional en ética digital. Se concluye con recomendaciones que son más puntuales para la academia, el gremio contable y las políticas públicas, orientadas a promover una cultura de innovación responsable, mejorando los controles de seguridad en la gestión financiera y actualizando las competencias del contador público para enfrentar cada uno de los retos de la era digital.

Palabras clave. Cibercontabilidad, Ética Profesional, Seguridad de la Información, Transformación Digital, Contabilidad 4.0, Costa Rica, Educación Contable.

CYBERACCOUNTING IN THE DIGITAL ERA: ETHICAL, TECHNICAL, AND INFORMATION SECURITY PERSPECTIVES IN COSTA RICA AND LATIN AMERICA

MAEd. Alejandro José Rodríguez Arguedas, alrodriguez@usam.ac.cr

Received: March 16, 2026

Accepted: May 22, 2026

Abstract. Digital accounting has become an emerging concept that integrates traditional accounting with digital technologies and cybersecurity. This article explores, from an academic perspective, the ethical, technical, and information security implications associated with the digital transformation of accounting, both in professional business practice and university teaching. Using a mixed methodology (quantitative and qualitative), the global and regional state of the art is analyzed, incorporating a case study applied in Costa Rica. The findings demonstrate that the rapid digitization of accounting raises ethical dilemmas (such as data confidentiality and algorithmic transparency), technical challenges (adoption of accounting 4.0, artificial intelligence, blockchain, and cloud computing), and significant cybersecurity risks to the protection of financial information. In the Costa Rican and Latin American context, a gap is observed between technological evolution and current regulatory frameworks, as well as a need to strengthen professional training in digital ethics. It concludes with more specific recommendations for academia, the accounting profession, and public policy, aimed at promoting a culture of responsible innovation, improving security controls in financial management, and updating the skills of public accountants to face each of the challenges of the digital age.

Keywords. Cyber accounting, Professional ethics, Information security, Digital transformation, Accounting 4.0, Costa Rica, Accounting education.

1. INTRODUCCIÓN

En las últimas décadas, la profesión contable ha experimentado una transformación profunda impulsada por la digitalización de procesos, la automatización y la globalización de los negocios. Este fenómeno, conocido en ocasiones como Contabilidad 4.0 o simplemente contabilidad digital, implica la integración de tecnologías avanzadas como la inteligencia artificial (IA), el big data, blockchain y sistemas en la nube en funciones que son más tradicionales de registro, análisis financiero y de auditoría. La promesa de estas tecnologías es una mayor eficiencia, precisión y rapidez en el procesamiento de la información financiera. Sin embargo, su adopción conlleva una serie de desafíos éticos y de seguridad que deben ser abordados para que se mantenga la integridad, la transparencia y la confiabilidad de la información contable.

Uno de los problemas centrales identificados es la aparición de nuevos riesgos y dilemas éticos asociados al uso de tecnología en contabilidad. Estudios recientes señalan la existencia de vacíos en los marcos normativos y deontológicos frente a las tecnologías emergentes: por ejemplo, la falta de transparencia en los algoritmos utilizados para análisis financiero automatizado, los riesgos para la confidencialidad de datos contables sensibles y la posible delegación excesiva de responsabilidades en sistemas

de IA sin supervisión humana adecuada. La rápida evolución tecnológica no siempre ha sido acompañada por actualizaciones proporcionales en los códigos de ética profesional o en la regulación, generando una desconexión entre la innovación y la normativa vigente. Este desfase plantea el riesgo de una eventual “desprofesionalización” del contador si sus funciones críticas son incluidas por sistemas automáticos y la subordinación de los principios éticos a lógicas puramente eficientes o comerciales. Por ello, organismos internacionales como la Junta Internacional de Ética para Contadores (IESBA, por sus siglas en inglés) han estudiado los impactos de tecnologías disruptivas (IA, blockchain, computación en nube, etc.) sobre la ética profesional, emitiendo recomendaciones para reforzar la confianza pública y adaptar el Código de Ética a estos nuevos desafíos.

Paralelamente, la seguridad de la información ha emergido como una preocupación de primera línea en el ámbito contable. Los sistemas contables digitales, al igual que otras infraestructuras críticas, se han vuelto objetivos recurrentes de ciberataques que pueden comprometer datos financieros, interrumpir operaciones e incluso erosionar la confianza en los informes financieros. Incidentes recientes han demostrado las graves consecuencias de las brechas de seguridad: por ejemplo, Costa Rica sufrió en 2022 una serie de ciberataques de tipo ransomware contra sistemas gubernamentales

(incluyendo el Ministerio de Hacienda), lo que obligó a desactivar las plataformas informáticas de recaudación tributaria y control aduanero, paralizando el comercio e impidiendo servicios en línea. Se estimaron pérdidas económicas cercanas a los \$30 millones diarios durante la interrupción de estas operaciones. La situación escaló al punto de declarar un estado de emergencia nacional por parte del Gobierno costarricense, al reconocer que estos ataques comprometían la continuidad del sector público y la seguridad económica del país. Este caso, que se analiza con mayor detalle más adelante, ejemplifica la vulnerabilidad de los sistemas contables y financieros ante amenazas cibernéticas sofisticadas, y subraya la urgencia de robustecer las defensas de ciberseguridad en entornos contables.

En el entorno latinoamericano y costarricense, la temática de la cibercontabilidad adquiere características particulares. Si bien la digitalización avanza en la región, existen brechas significativas en recursos tecnológicos, capacitación y concienciación sobre seguridad. Por ejemplo, Costa Rica ha impulsado la modernización de sus procesos contables y fiscales a través de la facturación electrónica obligatoria desde 2018, lo que marcó un hito en la transformación digital empresarial y tributaria del país. No obstante, junto a estos avances, persisten desafíos como la limitada inversión en ciberseguridad en muchas organizaciones, la escasez de

profesionales con competencias tecnológicas avanzadas, y un marco legal en evolución (leyes de protección de datos personales y normativa de delitos informáticos) que busca ponerse al día con las amenazas emergentes.

2. TESIS

Desde una perspectiva académica latinoamericana crítica, autores contemporáneos enfatizan la necesidad de analizar estos fenómenos considerando las realidades locales y las implicaciones socioeconómicas. Se plantea que la adopción acrítica de tecnologías desarrolladas en otros contextos puede no garantizar ni la ética ni la seguridad en nuestra región, si no se adapta a las condiciones culturales, educativas y regulatorias propias. En respuesta, han surgido iniciativas para “latinamericanizar” la discusión, incorporando visiones decoloniales y reflexivas sobre cómo la contabilidad digital puede servir al interés público en América Latina, evitando reproducir desigualdades o dependencias tecnológicas externas. Esto implica, por ejemplo, fomentar una perspectiva ética latinoamericana que priorice la transparencia, la justicia y la inclusión digital, así como investigaciones locales que documenten casos, brechas y mejores prácticas en nuestros países.

Planteamiento del problema: considerando lo anterior, el problema investigativo que aborda

este artículo es cómo equilibrar e integrar adecuadamente las dimensiones éticas, técnicas y de seguridad de la información en la práctica contable digital, de modo que la profesión contable pueda aprovechar las ventajas de la tecnología sin menoscabo de sus valores fundamentales ni de la confianza pública. Este problema se manifiesta en preguntas concretas tales como: ¿Están los contadores y las empresas preparados para mitigar los riesgos cibernéticos asociados a la contabilidad electrónica? ¿Cómo se están formando los futuros contadores en las competencias digitales y éticas que exige la era de la información? ¿Qué lecciones aporta el caso costarricense al debate global sobre ciberseguridad contable?

3. ARGUMENTOS

Desafíos éticos en la era de la cibercontabilidad

La ética profesional en contabilidad siempre ha enfatizado valores como la integridad, objetividad, confidencialidad, competencia y comportamiento profesional. Estos principios están recogidos en códigos de ética internacionales (el Código de Ética de la IESBA) y nacionales (como el Código de Ética Profesional del Contador Público Autorizado en Costa Rica). Con la entrada de las tecnologías digitales en el ejercicio contable, dichos principios enfrentan nuevos

contextos y situaciones límite que requieren interpretación y, en algunos casos, ampliación o ajuste de las normas deontológicas.

Uno de los dilemas éticos más citados es el de la transparencia algorítmica. Cuando las decisiones contables o financieras (por ejemplo, detección de fraudes, evaluación crediticia, estimaciones contables) son asistidas por algoritmos de IA o aprendizaje automático, surge la pregunta de cómo asegurar que dichos algoritmos operen bajo criterios justos, verificables y alineados con los valores de la profesión. Hurtado-Guevara et al. (2023), tras una revisión sistemática de literatura entre 2015 y 2024, señalan que la “falta de transparencia algorítmica” es un problema ético relevante: los contadores pueden verse utilizando herramientas cuyo funcionamiento no comprenden del todo, lo que dificulta identificar sesgos o errores y diluye la responsabilidad profesional. Asociado a esto está la delegación indebida de responsabilidades a sistemas automatizados: confiar ciegamente en un software para decisiones que afectan la razonabilidad de los estados financieros puede contravenir el principio de diligencia y escepticismo profesional. En ningún caso la tecnología debe convertir al contador en un “operador pasivo”; por el contrario, el profesional sigue siendo responsable de los reportes emitidos, y éticamente debe asegurar que entiende y supervisa las herramientas que utiliza.

Otro frente ético crítico es el de la confidencialidad y privacidad de la información. La contabilidad maneja datos sensibles de personas y empresas (ingresos, propiedades, estrategias fiscales, etc.), cuya divulgación no autorizada puede tener implicaciones legales y reputacionales. En entornos digitales, estos datos están almacenados en sistemas que pueden ser objeto de intrusiones o fugas. La ética en cibercontabilidad demanda no solo la obligación tradicional de guardar secreto profesional, sino también la proactividad en proteger los datos mediante buenas prácticas de seguridad (encriptación, controles de acceso) y el cumplimiento de marcos legales de protección de datos personales. En Latinoamérica, varios países han legislado en años recientes para tutelar la privacidad (por ejemplo, la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales en Costa Rica, la Ley General de Protección de Datos de Brasil, las normativas de habeas data en países andinos, etc.). Estas leyes exigen a los contadores, en tanto custodios de información financiera personal, un deber ético-jurídico de resguardo de dichos datos. Además, plantean el principio de minimización de datos, es decir, recolectar y conservar solo la información necesaria y durante el tiempo requerido, algo que también desafía la mentalidad tradicional de “guardar todo” en contabilidad.

La independencia y objetividad del

profesional contable enfrenta asimismo retos sutiles en la era digital. Por ejemplo, el uso de herramientas de big data y analítica puede exponer al contador a informaciones adicionales (trends de mercado, redes sociales, etc.) que podrían sesgar su juicio al preparar proyecciones o estimaciones contables. O la adopción de software patrocinado por ciertas empresas tecnológicas podría generar conflictos de interés si el profesional se vuelve dependiente de un solo proveedor. Aquí, la ética requiere mantener la objetividad y la independencia mental, más allá de las influencias de la tecnología empleada. La competencia profesional es otro principio que cobra nueva vida: los contadores ahora tienen la obligación ética de “mantener sus conocimientos y habilidades al día” no solo en normativa contable sino en materia tecnológica. No estar actualizado en tendencias como ciberseguridad o sistemas de información podría implicar una falta ética por negligencia, ya que se expondría la información de clientes o se brindaría un servicio inferior al estándar esperado en la actualidad.

Hurtado-Guevara et al. (2023) concluyen que existe una brecha formativa importante en ética digital dentro de la profesión contable. Muchos contadores en ejercicio y estudiantes de contaduría no han recibido educación suficiente sobre cómo aplicar los principios éticos en contextos de sistemas informáticos, inteligencia artificial o redes sociales.

Este vacío educativo puede traducirse en comportamientos poco éticos (aunque sea por desconocimiento) como, por ejemplo, el uso inadecuado de datos masivos, la falta de atención a alertas de ciberseguridad, o la adopción de tecnologías sin evaluar sus implicaciones éticas. La discusión académica latinoamericana advierte incluso que, de no tomar acciones, podríamos ver una subordinación de la ética a la eficiencia tecnológica —es decir, priorizar la rapidez y conveniencia de la automatización por encima de los valores éticos y del juicio profesional crítico— lo cual sería altamente perjudicial para la credibilidad de la información financiera.

Afortunadamente, se vislumbran soluciones y esfuerzos en marcha para afrontar estos desafíos éticos. A nivel global, la IESBA emitió en 2022 un informe final con recomendaciones concretas para incorporar en el Código de Ética temas relacionados con tecnología. Entre las recomendaciones está clarificar la responsabilidad del profesional en la utilización de outputs de IA, fortalecer las guías sobre confidencialidad de información en entornos en la nube, y promover principios de transparencia en la divulgación de uso de expertos o sistemas en la realización de tareas profesionales. A nivel local, los colegios y asociaciones contables de la región han comenzado a difundir guías de buenas prácticas. Por ejemplo, el Instituto Mexicano de Contadores Públicos (IMCP) ha enfatizado

la necesidad de fortalecer las competencias digitales del gremio, no solo técnicas sino también éticas, instando a sus miembros a capacitarse en el manejo responsable de tecnologías. De igual forma, en Colombia, la Junta Central de Contadores ha incluido contenidos sobre ética y TIC en sus programas de desarrollo profesional continuo.

En Costa Rica, el Colegio de Contadores Públicos ha reconocido los riesgos del uso de herramientas tecnológicas sin la debida preparación ética y técnica, advirtiendo a sus agremiados sobre, por ejemplo, el uso de inteligencia artificial en la elaboración de informes financieros, que, si bien puede acelerar ciertas tareas, no exime al profesional de su juicio y responsabilidad éticos. Iniciativas de formación en ética informática y cibernética (ética aplicada a entornos cibernéticos) están surgiendo en las universidades y colegios profesionales del país, como parte de la respuesta a esta necesidad.

En resumen, la cibercontabilidad desafía a la profesión contable a reafirmar y adaptar sus valores éticos en un mundo digital. Los principios tradicionales siguen siendo válidos, pero deben interpretarse en contextos nuevos. La profesión debe rechazar firmemente la idea de que “la tecnología lo hace todo” y, en cambio, abrazar una cultura ética digital, donde la tecnología sea utilizada como herramienta bajo la supervisión y criterio del

contador, manteniendo siempre la primacía del interés público, la transparencia y la calidad de la información financiera.

Seguridad de la información y ciberseguridad en la contabilidad

La seguridad de la información es un pilar intrínseco de la cibercontabilidad, dado que la confianza en los informes financieros depende de la integridad, disponibilidad y confidencialidad de los datos que los sustentan. En la era digital, estas propiedades deben garantizarse frente a un abanico creciente de amenazas cibernéticas. Entre las principales amenazas que enfrentan los sistemas contables digitalizados se encuentran: el malware (software malicioso, incluyendo virus, ransomware y spyware), las intrusiones no autorizadas (ataques de hackers buscando robar o alterar información), el phishing dirigido al personal contable (engaños por correo electrónico para obtener credenciales o pagos fraudulentos) y las fallas o sabotajes internos (empleados o exempleados que abusan de su acceso a los sistemas).

Un estudio empírico reciente realizado en Ecuador por Calle-Tenesaca y Andrade-Amoroso (2024) examinó la exposición a riesgos cibernéticos en empresas comerciales y las medidas de mitigación tomadas por sus áreas contables. Entre sus hallazgos destaca que “las amenazas más comunes

incluyen intrusiones internas y malware” en los sistemas financieros, y si bien la mayoría de empresas encuestadas reportó realizar actualizaciones de software y capacitación de personal en seguridad informática, persistía “preocupación por la preparación ante amenazas cibernéticas y una asignación limitada de presupuesto para ciberseguridad”. En particular, se identificaron debilidades en la implementación de controles internos de seguridad y la necesidad de mayor inversión en tecnología de protección. Estas conclusiones reflejan una realidad extendida en Latinoamérica: muchas organizaciones (en especial Pymes) aún destinan recursos insuficientes para proteger sus datos contables, subestimando el impacto potencial de los incidentes de seguridad.

La situación antes descrita se vio dramáticamente ilustrada por el caso de Costa Rica 2022 mencionado en la introducción. El ataque del grupo Conti afectó sistemas claves como la plataforma TICA de aduanas y el portal ATV de administración tributaria, dejando inoperantes servicios durante semanas. Como resultado, trámites que normalmente se realizaban en línea tuvieron que revertirse a procesos manuales, generando cuellos de botella en la administración pública, parálisis temporal del comercio exterior y perjuicios económicos sustanciales. Este incidente reveló que incluso un país catalogado de ingreso medio alto como Costa Rica puede

ser altamente vulnerable si no cuenta con una estrategia robusta de ciberseguridad a nivel estatal y empresarial. De hecho, expertos locales señalaron que lo ocurrido marcó “el comienzo de una era de ciberataques sin precedentes”, instando a aprender la lección y mejorar la resiliencia digital. Tras los ataques, se reforzaron las alianzas internacionales para recibir asistencia técnica en la recuperación de sistemas y se aceleró la discusión de una estrategia nacional de ciberseguridad.

En el ámbito corporativo privado, la seguridad de la información contable implica establecer un sistema de control interno enfocado en TI. Tradicionalmente, el control interno en contabilidad se ha preocupado de salvaguardar activos, separar funciones, asegurar registros fidedignos, etc. Ahora, a eso se suma garantizar que los sistemas informáticos contables tengan medidas de seguridad como: autenticación robusta de usuarios (múltiple factor de autenticación), roles y privilegios correctamente asignados (para que cada usuario solo acceda a lo necesario), cifrado de datos sensibles en bases de datos y respaldos, monitoreo activo de accesos y transacciones inusuales, firewalls y antivirus actualizados, planes de continuidad del negocio y respaldo de información (copias de seguridad periódicas protegidas contra ransomware), entre otros. Un elemento crítico es la ciber higiene del personal: así como se entrena a los empleados en ética, también deben entrenarse en prácticas seguras, por

ejemplo, reconocer intentos de phishing, usar contraseñas seguras, no instalar software no autorizado, respetar las políticas de la empresa sobre uso de dispositivos USB, etc. La cultura de seguridad es tanto o más importante que la tecnología implementada.

Como parte de la respuesta internacional, instituciones como la Federación Internacional de Contadores (IFAC) han enfatizado la relevancia de que los contadores adquieran conocimientos básicos en ciberseguridad y colaboren estrechamente con los departamentos de TI en la gestión de riesgos. En una entrevista de IFAC, Oppenheim y Brinich (2023) recalcan que “no es cuestión de si [una empresa] sufrirá un ciberataque, sino cuándo”, y que los contadores, al manejar información financiera sensible, deben saber salvaguardar esos datos y apoyar la mitigación de riesgos en toda la organización. De hecho, la gestión efectiva de sistemas de control interno hoy día incluye la prevención y detección de intrusiones cibernéticas como parte del rol del contador de gestión en conjunto con TI. Los contadores, por su formación, aportan fuertes habilidades analíticas que les permiten dimensionar riesgos y proponer controles; tradicionalmente han sido garantes de la fidelidad de la información, y esa responsabilidad ahora abarca también la seguridad de la información.

Normativamente, los estándares de auditoría

financiera han incorporado consideraciones explícitas sobre riesgos de TI. Por ejemplo, la Norma Internacional de Auditoría (NIA) 315 revisada exige a los auditores comprender el entorno de TI de la entidad y considerar riesgos derivados de este, incluyendo riesgos de ciberseguridad, al identificar riesgos de declaración equivocada material. Ignorar la posibilidad de fraudes o errores debido a ataques informáticos sería una deficiencia en la planificación de la auditoría. En consecuencia, hoy es común que las firmas de auditoría incluyan especialistas en TI (auditores de sistemas) en sus equipos, o que utilicen herramientas informáticas en la selección de muestras y pruebas de control generales de TI.

En Latinoamérica, diversas iniciativas buscan mejorar la postura de seguridad en el ámbito contable y financiero. Países como Chile, México, Colombia y el propio Costa Rica han emitido en los últimos años guías o normas sectoriales sobre ciberseguridad en entidades financieras, algunas de las cuales son aplicables indirectamente a departamentos de contabilidad (por ejemplo, regulaciones sobre protección de información financiera de clientes, que deben observar también las áreas contables al manejar datos). Además, la Asociación Interamericana de Contabilidad (AIC) ha desarrollado seminarios y documentos técnicos para sensibilizar a los contadores de la región sobre la ciberseguridad. Un documento de AIC destaca

que “la contabilidad está experimentando una transformación significativa... en América Latina, los contadores deben asumir un papel activo frente al desafío de la ciberseguridad, actualizándose y compartiendo responsabilidad con las áreas de TI”. Esto resalta que la ciberseguridad no puede delegarse únicamente al personal técnico; dado que los procesos contables son los que podrían verse afectados, los contadores deben involucrarse en su protección.

Algunas buenas prácticas propuestas específicamente para contabilidad y auditoría incluyen: realizar auditorías informáticas preventivas (simular ataques o evaluar vulnerabilidades en los sistemas contables antes de que ocurran incidentes); implementar controles automatizados dentro de los software contables (por ejemplo, alertas cuando se modifica un asiento histórico, o límites para transacciones inusuales); establecer planes de respuesta a incidentes que contemplen la continuidad de las operaciones contables (¿cómo facturar o pagar nómina si el sistema está caído? hay que tener procedimientos alternos); y, muy importante, adquirir ciberseguros cuando sea pertinente, para transferir parcialmente el riesgo financiero de ciertos ataques.

4. CONCLUSIONES

En conclusión, la seguridad de la información en cibercontabilidad es un componente no negociable para salvaguardar la calidad y confianza de la información financiera. Un sistema contable digitalmente avanzado pero inseguro es una paradoja peligrosa. Por ello, la evolución hacia la contabilidad digital debe ir acompañada de una evolución paralela en los mecanismos de seguridad y en la conciencia tanto de contadores como de sus clientes y organizaciones acerca de la ciber-resiliencia. La lección de casos como el de Costa Rica es clara: invertir en ciberseguridad es invertir en la continuidad del negocio y en la confianza del mercado. La siguiente sección abordará cómo estas dimensiones éticas, técnica y de seguridad se integran en la práctica mediante la metodología de investigación adoptada y el estudio de caso en Costa Rica.

Perspectiva latinoamericana y contexto costarricense

Si bien los grandes temas de la cibercontabilidad (digitalización, ética, seguridad) son globales, es crucial analizarlos bajo la perspectiva latinoamericana, incorporando voces de autores y realidades de la región. Latinoamérica presenta contextos socioeconómicos diversos, con contrastes entre países más avanzados tecnológicamente y otros rezagados, pero comparte ciertos desafíos históricos:

limitaciones presupuestarias en instituciones, desigualdades en acceso a la tecnología, marcos legales en desarrollo y, en el ámbito contable, una profesión que ha ido adoptando estándares internacionales (IFRS, ISA) pero que enfrenta el reto de adaptar la formación y el ejercicio a las demandas tecnológicas actuales.

Una aportación característica de la perspectiva latinoamericana es la mirada crítica y contextual. Por ejemplo, autores como Salcedo (2021) y Tapia (2022) – representando la llamada “contabilidad crítica” en la región– argumentan que la transformación digital debe evaluarse no solo en términos de eficiencia empresarial, sino también en cómo impacta a las personas (trabajadores contables, estudiantes, pequeños empresarios) y a la soberanía tecnológica de nuestros países. Existe el riesgo, señalan, de una dependencia tecnológica de soluciones importadas (software de contabilidad extranjeras, servicios en la nube de corporaciones globales) sin desarrollo local, lo cual puede generar vulnerabilidades estratégicas y transferencia inadvertida de datos sensibles fuera de jurisdicciones nacionales. Este enfoque crítico invita a impulsar la innovación regional en cibercontabilidad (desarrollo de software contable local, normativas de localización de datos) y a incluir en las decisiones éticas consideraciones de equidad (por ejemplo, cómo la automatización afecta el empleo

contable en la región, o cómo proteger a poblaciones contables de menores recursos frente al ciberdelito).

En Costa Rica, el contexto de cibercontabilidad viene marcado por un sector de servicios financieros relativamente desarrollado, una alta penetración de Internet y una institucionalidad sólida, pero también por brechas en ciberseguridad evidenciadas recientemente. El país cuenta con un Colegio de Contadores Públicos que ha ido incorporando capacitaciones en NIIF electrónicas, facturación digital y recientemente en protección de datos y ciberseguridad. Universidades públicas y privadas han actualizado sus currículos de contaduría para incluir cursos de sistemas de información contable, auditoría informática e incluso certificaciones internacionales (como MOS, SAP, etc.) para sus estudiantes. A nivel de política pública, Costa Rica promulgó en 2011 la Ley 9048 de Delitos Informáticos y en 2019 actualizó su Estrategia Nacional de Ciberseguridad, creando el CSIRT (Equipo de Respuesta a Incidentes de Seguridad) nacional, lo que provee un marco dentro del cual se manejan incidentes que pueden afectar a múltiples sectores, incluido el financiero-contable.

Un componente singular del contexto costarricense es la fuerte interrelación entre contabilidad gubernamental y digitalización. El Gobierno Digital ha impulsado sistemas

como el SICOP (para compras públicas) y el SIGAF (para la gestión financiera pública) que integran de manera electrónica las operaciones contables del Estado. Esto es positivo en transparencia y eficiencia, pero también convierte a la hacienda pública en un objetivo atractivo para ciberataques motivados políticamente o por lucro (como fue el caso del ransomware que cifró datos del Ministerio de Hacienda en 2022). Por tanto, la contabilidad pública costarricense se ha visto obligada a adoptar estándares de ciberseguridad a la par de su modernización (ej.: el Ministerio de Hacienda fortaleciendo sus respaldos externos y protocolos de recuperación tras el ataque). Este caso costarricense sirve de estudio de caso no solo local sino regional, pues otros países han tomado nota de la experiencia para revisar sus medidas de seguridad en las tesorerías y administraciones tributarias.

Desde la mirada latinoamericana, también es menester resaltar enfoques de contabilidad social y ética latinoamericana que se preguntan cómo la tecnología puede ser un habilitador para mejores prácticas de transparencia y rendición de cuentas. Por ejemplo, en países con problemas de corrupción, la implementación de sistemas contables digitales con trazabilidad (incluso mediante blockchain) podría dificultar la manipulación de cuentas públicas. Costa Rica, con un índice de transparencia relativamente alto en la región, podría liderar en la adopción

de tecnologías para garantizar la pureza de los registros contables públicos y privados. Sin embargo, ello requiere marcos éticos robustos: que el afán de modernización no atropelle principios de participación o control ciudadano. La perspectiva latinoamericana crítica sugiere incluir en los procesos de digitalización a las comunidades profesionales locales, a la academia y a la sociedad civil, para lograr soluciones pertinentes.

Finalmente, es relevante mencionar la cooperación regional. Latinoamérica, frente a amenazas comunes (fraudes financieros transnacionales, ciberataques a bancos centrales, etc.), ha comenzado a formar redes de colaboración. En contabilidad, la AIC agrupa colegios de contadores de casi todos los países de la región y ha propiciado intercambios en materia de tecnología. Costa Rica, por medio de convenios con otros países y organismos internacionales (como el BID o la OEA), ha participado en proyectos para mejorar la ciberresiliencia de sus instituciones financieras. Estas colaboraciones permiten compartir mejores prácticas, alertas tempranas de amenazas y hasta ejercicios conjuntos de seguridad. Una visión latinoamericanista de la cibercontabilidad promueve precisamente esa solidaridad regional en la capacitación y defensa contra riesgos cibernéticos, entendiendo que los delitos informáticos no respetan fronteras.

En síntesis, la perspectiva latinoamericana

aporta un enfoque holístico que complementa los desarrollos globales de la cibercontabilidad. Contextualiza los principios a nuestra realidad, advierte sobre riesgos específicos (brechas digitales, dependencias tecnológicas) y orienta las soluciones hacia la inclusión, la soberanía y la cooperación. El caso costarricense, con sus avances y lecciones aprendidas, se convierte en un aporte valioso a la región. Sobre esta base teórica, en la siguiente sección se describen la metodología empleada en la presente investigación para articular todos estos elementos y los detalles del estudio de caso aplicado.

Cibercontabilidad en la docencia universitaria

Un eje central para lograr que la cibercontabilidad sea exitosa en la práctica es la formación académica de los futuros contadores. Las universidades y centros de formación profesional tienen el reto de actualizar sus planes de estudio para incluir las competencias digitales y conocimientos interdisciplinarios que el mercado y la sociedad demandan. En Costa Rica y Latinoamérica, la docencia universitaria en contaduría ha ido incorporando gradualmente cursos y contenidos relacionados con sistemas de información contable, herramientas tecnológicas (como Excel avanzado, software ERP) y auditoría de TI. No obstante, según diversos diagnósticos, aún existe un camino

por recorrer para integrar plenamente las temáticas de ciberseguridad, analítica de datos y ética tecnológica en el currículo contable.

A raíz de la pandemia de COVID-19 (2020-2021), muchas facultades de ciencias económicas en la región aceleraron la virtualización y el uso de plataformas digitales, lo cual puso de relieve la necesidad de competencias digitales tanto en docentes como en estudiantes de contabilidad. Un estudio sobre educación contable en la era digital (Jubones et al., 2021) reveló que la tecnología está “transformando profundamente la formación contable, permitiendo la personalización del aprendizaje” y ampliando las herramientas a disposición, pero que persisten brechas en el acceso y en la capacitación pedagógica para su uso. En Costa Rica, universidades como la Universidad de Costa Rica (UCR) y el Instituto Tecnológico de Costa Rica (ITCR) han incorporado laboratorios de software contable, simuladores de negocios digitales e incluso componentes de programación básica en algunas maestrías de gestión contable. Esto apunta en la dirección correcta.

La educación en ciberseguridad para contadores es un aspecto neurálgico. Tradicionalmente, la seguridad informática se veía como dominio exclusivo de ingenieros en sistemas. Sin embargo, hoy se reconoce que los contadores deben al menos comprender

los principios básicos (por ejemplo, qué es encriptación, qué son controles de acceso, cómo identificar un correo malicioso, etc.) para poder desempeñar su rol sin exponer información sensible. IFAC reporta que a nivel global “los académicos están trabajando para preparar a los estudiantes para el nuevo entorno laboral... exponiendo a los estudiantes a los avances tecnológicos y los riesgos correspondientes es de alta prioridad”. Muchas universidades en el mundo han respondido agregando asignaturas de analítica de datos y TI aplicada a contabilidad, que suelen incluir módulos de evaluación de riesgos y fraude digital. Este modelo está siendo replicado en Latinoamérica: por ejemplo, en Perú una universidad integró en su curso de Contabilidad Computarizada no solo el uso de software sino la reflexión sobre la ética y seguridad en entornos digitalizados (Castillo, 2023).

En Costa Rica, la formación de contadores públicos autorizados exige cumplir con horas de educación continua anualmente. El Colegio de Contadores ha comenzado a ofrecer dentro de esa oferta de educación continua charlas y cursos sobre “Controles Internos y Ciberseguridad para Contadores”, “Normativa de Protección de Datos Personales y su impacto en la Auditoría”, entre otros. Asimismo, se ha evidenciado un creciente interés de estudiantes por proyectos de graduación relacionados con TI; por ejemplo, tesis sobre la implementación de

sistemas contables en la nube para Pymes, o sobre análisis forense digital aplicado a investigaciones de fraudes contables. Estas son señales positivas de que la academia costarricense está respondiendo a la evolución del perfil profesional.

Autores latinoamericanos abogan por un rediseño curricular integral. Hurtado-Guevara et al. (2023) concluyen en su estudio que es “urgente actualizar los códigos de ética profesional, rediseñar la formación académica y promover una cultura crítica” en la formación de contadores, para gestionar la innovación tecnológica de manera ética y sostenible. Es decir, se propone no solo añadir cursos sueltos, sino repensar toda la malla curricular bajo una visión que integre contabilidad, administración, tecnología y humanismo. Algunos elementos sugeridos para esta integración incluyen: aprendizaje basado en proyectos de sistemas de información reales; colaboración interdisciplinaria con estudiantes de informática o ingeniería en proyectos comunes (por ejemplo, desarrollar juntos un pequeño sistema contable); simulaciones de ciberataques en contextos contables para aprender respuestas; debate de casos éticos sobre IA en contabilidad; e incorporación de certificaciones internacionales (como la Certificación en Ciberseguridad y Prácticas de Datos que ofrece la IMA, mencionada por Oppenheim, 2023) como parte del programa.

Un ejemplo de mejora curricular lo brinda la Universidad Intercontinental de México (Perez Herrera, 2025), donde la Licenciatura en Contaduría y Finanzas incorpora desde los primeros semestres contenidos en tecnologías de la información, auditoría digital y gestión de riesgos, con un enfoque integral y docentes especializados. Programas similares podrían adaptarse al contexto costarricense, aprovechando nuestra tradición educativa de calidad. Además, entes como la Agencia Nacional de Acreditación (SINAES, en Costa Rica) podrían actualizar sus criterios de evaluación de carreras de contaduría para incluir la pertinencia tecnológica.

Finalmente, cabe destacar que la docencia universitaria en cibercontabilidad no solo beneficia a los estudiantes, sino que puede irradiar hacia la profesión en general a través de la extensión y educación continua. Universidades pueden ofrecer diplomados o cursos abiertos en contabilidad digital para profesionales ya graduados, o asesorar a empresas en implementación de buenas prácticas. La convergencia de academia, sector privado y organismos profesionales en eventos, congresos y publicaciones sobre estos temas es sumamente valiosa para difundir el conocimiento. En Costa Rica, la Universidad de Costa Rica y la Universidad Nacional han organizado en conjunto con el Colegio de Contadores Públicos simposios

sobre Tecnología y Contabilidad que abordan temas de Fintech, ciberseguridad y analítica, reflejando la importancia de estas alianzas.

En resumen, la docencia universitaria en contabilidad enfrenta el desafío impostergable de formar contadores competentes digitalmente y conscientes éticamente. Los avances ya iniciados deben profundizarse y sistematizarse, de forma que los egresados costarricenses y latinoamericanos salgan preparados no solo para llevar libros, sino para gestionar sistemas, proteger datos y guiar a sus organizaciones en un entorno digital complejo. La siguiente sección presentará la metodología empleada en esta investigación, la cual busca precisamente articular una mirada teórico-empírica sobre cómo la práctica contable y la enseñanza contable están abordando (o deberían abordar) estos retos.

5. CITAS Y REFERENCIAS BIBLIOGRÁFICAS

Calle-Tenesaca, M. E., & Andrade-Amoroso, R. P. (2024). Ciberseguridad en contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales. *Revista Metropolitana de Ciencias Aplicadas*, 7(S2), 56–71. <https://doi.org/10.62452/bdc3pg66>

Deloitte México. (2025). *El perfil contable en la era digital*. [Informe no publicado, citado en Pérez Herrera, 2025].

Hurtado-Guevara, R. F., Almeida-Blacio, J. H., & López-Pérez, P. J. (2023). Desafíos éticos en la adopción de tecnologías emergentes en contabilidad. *Revista Científica Ciencia y Método*, 1(2), 29–42. <https://doi.org/10.55813/gaea/rcym/v1/n2/13>

International Ethics Standards Board for Accountants (IESBA). (2022). *Technology: Ethics and Independence Considerations* (Phase 2 Final Report). IESBA.

International Federation of Accountants (IFAC). (2023, October 11). *Why professional accountants need to care about cybersecurity* [Entrevista de J. Oppenheim & A. Brinich]. IFAC Knowledge Gateway. <https://www.ifac.org/knowledge-gateway/discussion/why-professional-accountants-need-care-about-cybersecurity>

Murillo, A. (2022, May 17). *Cyber attack on Costa Rica grows as more agencies hit, president says*. Reuters News. <https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/>

- Pérez Herrera, D. (2025, July 8). *Ciberseguridad en contaduría, riesgo clave del siglo XXI*. Blog de la Universidad Intercontinental (UIC), México. <https://www.uic.mx/ciberseguridad-en-contaduria-riesgo-clave-del-siglo-xxi/>
- Rosch, C. (2022, June 1). *A massive cyberattack in Costa Rica leaves citizens hurting*. Rest of World. <https://restofworld.org/2022/cyberattack-costa-rica-citizens-hurting/>
- Vargas Luna, B., Ávila Padilla, F. A., & Martínez Sánchez, E. R. (2024). *Explorando las implicaciones de la tecnología 4.0 en la contabilidad: una revisión sistemática de la literatura*. [Tesis de pregrado, Universidad Cooperativa de Colombia]. Repositorio UCC <https://hdl.handle.net/20.500.12494/55617>