

The impact of Internal Control in ERP Systems on the financial reliability for Pymes' access to the Ecuadorian stock market

Amalia Mariuxi Aguay Tomalá ^{1,2} ; Glen Freddy Robayo Cabrera ^{1,3} ; Mercedes Johanna Espinoza Espinoza ^{1,4} ; Iván Alberto Illescas Rendón ^{1,5} 

¹Universidad Bolivariana del Ecuador, amaguayt@ube.edu.ec; gfrabayoc@ube.edu.ec; glenroca@alumni.uv.es; mjespinozac@ube.edu.ec; iaillascasr @ube.edu.ec
Universidad Bolivariana del Ecuador(UBE) Duran Ecuador

Abstract— This study analyzes the integration of internal control and auditing as strategic pillars for strengthening the management of technological innovation projects in Ecuador, focusing on the implementation of digital accounting systems. Despite the accelerated adoption of ERP systems driven by the 2022-2025 Digital Transformation Agenda, a critical gap exists between technical innovation and control mechanisms, increasing vulnerability to fraud and operational errors. The analysis, based on a sample of 138 professionals, reveals that 48.6% lack a formal risk assessment (combining informal assessments of 28.3% with a complete absence of assessments of 20.3%), reducing the process to a purely technical change. A key finding is the weakness of the human factor: 65.2% of staff received less than five days of training, leading to a low perception of self-efficacy and neutralizing the potential of the technological tools. This lack of coordination means that, even though 83.3% of organizations have digital controls in place, audit findings and regulatory issues persist with oversight bodies due to users' lack of technical knowledge. In conclusion, the success of accounting digitization depends not only on the software itself, but also on a comprehensive management model that applies the COSO and COBIT frameworks, prioritizing specialized training and preventive auditing to ensure financial integrity and organizational transparency.

Keywords— Internal control (COSO), ERP systems, Risk management, Technical training, Digital.

El impacto del Control Interno en Sistemas ERP sobre la fiabilidad financiera para el acceso de las PYMES al mercado bursátil ecuatoriano

Amalia Mariuxi Aguay Tomalá ^{1,2}; Glen Freddy Robayo Cabrera ^{1,3}; Mercedes Johanna Espinoza Espinoza ^{1,4}; Iván Alberto Illescas Rendón ^{1,5}

¹Universidad Bolivariana del Ecuador, amaguayt@ube.edu.ec; gfrabayoc@ube.edu.ec; glenroca@alumni.uv.es; mjespinozac@ube.edu.ec; iaillascasr @ube.edu.ec
Universidad Bolivariana del Ecuador(UBE) Durán Ecuador

Resumen— Este estudio analiza la integración del control interno y la auditoría como ejes estratégicos para el fortalecimiento de la gestión de proyectos de innovación tecnológica en Ecuador, centrándose en la implementación de sistemas contables digitales. A pesar de la acelerada adopción de sistemas ERP impulsada por la Agenda de Transformación Digital 2022-2025, existe una brecha crítica entre la innovación técnica y los mecanismos de control, lo que incrementa la vulnerabilidad ante fraudes y errores operativos. El análisis, basado en una muestra de 138 profesionales, revela que el 48.6% carecen de evaluación formal (sumando evaluaciones informales 28.3% más ausencia total 20.3%) de las implementaciones carecen de una evaluación de riesgos formal previa, reduciendo el proceso a un cambio meramente técnico. Un hallazgo determinante es la debilidad del factor humano: el 65.2% del personal recibió menos de cinco días de capacitación, lo que genera una baja percepción de autoeficacia y neutraliza la potencia de las herramientas tecnológicas. Esta desarticulación provoca que, aunque el 83.3% de las organizaciones cuente con controles digitales configurados, persistan hallazgos de auditoría y problemas regulatorios ante organismos de control por desconocimiento técnico del usuario. En conclusión, el éxito de la digitalización contable no depende exclusivamente del software, sino de un modelo de gestión integral que aplica los marcos COSO y COBIT, priorizando la formación especializada y la auditoría preventiva para garantizar la integridad financiera y la transparencia organizacional.

Palabras Claves: Control interno(COSO), Sistemas ERP, Gestión de riesgos, capacitación técnica, Transformación.

I. INTRODUCCIÓN

La transformación digital ha reconfigurado el ecosistema empresarial en Ecuador, alterando profundamente los procesos contables y de gestión financiera. Entre 2020 y 2025, la adopción de sistemas de Planificación de Recursos Empresariales (ERP) como SAP, Fitbank y Oracle, el análisis de casos en nube, ha experimentado una aceleración sin precedentes, impulsada tanto por la búsqueda de eficiencia operativa como por marcos normativos como la Agenda de Transformación Digital del Ecuador 2022-2025 [1] y [2].

A pesar de los beneficios documentados en términos de reducción de costos y optimización estratégica [3] la celeridad

de esta transición ha generado una brecha crítica: la desarticulación entre la innovación tecnológica y los mecanismos de control interno. Esta problemática se manifiesta en la implementación de herramientas digitales sin una evaluación de riesgos previa, lo que incrementa la vulnerabilidad ante errores operativos y fraudes [4]. La falta de una cultura de innovación integrada —agravada por la limitada vinculación entre la academia, el Estado y el sector productivo [5] — sitúa a las organizaciones en un escenario de riesgo regulatorio y operativo frente a organismos de control como el Superintendencia de Compañías Valores y Seguros, Servicio de rentas internas, y la Superintendencia de Economía Popular y Solidaria.

El control interno y el marco COSO en la era digital, no debe entenderse como un proceso estático, sino como un sistema dinámico. En el ámbito de los ERP, la configuración de controles digitales —como la segregación de funciones automatizada y los niveles de autorización electrónicos— es esencial para mitigar los registros inadecuados identificados por [6]. El marco COSO proporciona la estructura necesaria para que la digitalización no comprometa la integridad de los estados financieros.

En Ecuador, el modelo COSO constituye la base conceptual para las Normas de Control Interno emitidas por la Contraloría General del Estado (CGE), aplicables a todas las entidades del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos [7]. Estudios recientes demuestran que las organizaciones ecuatorianas han adoptado el marco COSO para la realización de operaciones y la implementación de medidas de control institucional [8].

La auditoría contemporánea ha evolucionado hacia el uso de inteligencia artificial y análisis de datos masivos. No obstante, la tecnología por sí sola es insuficiente si no va acompañada de un cambio cultural organizacional [9]. La literatura reciente sugiere que la insuficiencia en los programas de capacitación es el principal obstáculo para que las

funcionalidades de control de los sistemas contables sean explotadas eficazmente [10].

La innovación tecnológica en instituciones de educación superior y empresas ecuatorianas enfrenta barreras estructurales. Según la SENESCYT, la concentración de capacidades en pocas regiones y la baja categorización de investigadores limitan la transferencia de conocimiento. La gestión de proyectos tecnológicos, por tanto, requiere un enfoque interdisciplinario que una la viabilidad técnica con la seguridad financiera y el cumplimiento normativo exigido por la Contraloría General del Estado.

La adopción de las Normas Internacionales de Información Financiera (NIIF) [11]. En Ecuador marcó un hito en la arquitectura contable nacional, transitando de las Normas Ecuatorianas de Contabilidad (NEC) hacia un marco de transparencia y comparabilidad global. Este proceso, regulado por la Superintendencia de Compañías Valores y Seguros bajo una implementación escalonada entre 2010 y 2012, no solo redefinió la presentación de estados financieros, sino que impuso desafíos técnicos disruptivos en la infraestructura digital de las organizaciones. La necesidad de gestionar valoraciones a valor razonable, trazabilidad de políticas y segregación de funciones ha forzado una reingeniería de los sistemas ERP, donde la brecha de capacitación del talento humano (55%) y la complejidad normativa emergen como los principales obstáculos para una transición efectiva [12] y [13].

Paralelamente, la gobernanza corporativa en los sectores público y privado ecuatoriano ha evolucionado hacia la integración de la auditoría interna como un pilar de aseguramiento estratégico y rendición de cuentas. Bajo las directrices de la Contraloría General del Estado y marcos internacionales, la gobernanza de proyectos tecnológicos demanda actualmente una alineación rigurosa entre la inversión en TI y los objetivos institucionales. No obstante, persiste una desarticulación crítica entre las áreas financieras y tecnológicas, caracterizada por la ausencia de métricas de retorno de inversión y una participación reactiva de la auditoría, lo que incrementa los riesgos operativos y regulatorios ante organismos como el SRI y la SEPS) [14]; y [15].

Finalmente, la gestión de proyectos de innovación tecnológica en el contexto ecuatoriano requiere un modelo integrador que converja los marcos de control interno (COSO), gobernanza de TI (COBIT) [16]; y estándares financieros (NIIF). Esta sinergia permite abordar de manera holística las dimensiones críticas de la problemática: desde la evaluación formal de riesgos y la configuración de controles preventivos en plataformas digitales, hasta la mitigación de hallazgos de auditoría mediante una cultura de capacitación continua. Esta convergencia normativa y operativa es la que garantiza que la transformación digital no sea solo un cambio de herramientas,

sino una evolución hacia la resiliencia y la transparencia organizacional.

El objetivo fundamental es analizar la integración del control interno y la auditoría como ejes estratégicos para el fortalecimiento de la gestión de proyectos de innovación tecnológica en Ecuador, centrándose en la implementación de sistemas contables digitales. Para ello, se propone determinar el rigor de las evaluaciones de riesgos previas a la adopción tecnológica, diagnosticar la suficiencia de la capacitación técnica proporcionada al personal y verificar la configuración de controles preventivos y delectivos en entornos ERP. Asimismo, el estudio busca categorizar las brechas de cumplimiento detectadas por entes reguladores y contrastar la percepción de autoeficacia del personal frente a la seguridad operativa, permitiendo así establecer una correlación directa entre la solidez del sistema de control y el éxito de la transformación digital en las organizaciones.

II. MATERIALES Y MÉTODOS

El estudio se desarrolló bajo un enfoque cuantitativo de alcance descriptivo y diseño transversal, empleando una encuesta estructurada aplicada a una muestra de 138 profesionales de contabilidad y auditoría en Ecuador vinculados a procesos de implementación de sistemas ERP. El instrumento de recolección de datos se validó para medir tres dimensiones operativas: la ejecución de evaluaciones de riesgos financieros, la extensión de los programas de capacitación técnica y el nivel de configuración de controles internos automatizados. El procesamiento de la información se realizó mediante estadística descriptiva, permitiendo caracterizar la relación entre la infraestructura tecnológica adoptada y el cumplimiento de los estándares de control y auditoría vigentes en el entorno empresarial ecuatoriano. El instrumento fue validado mediante juicio de dos expertos: un magíster en contabilidad y finanzas, y un auditor certificado en marco COSO, quienes evaluaron la pertinencia, claridad y suficiencia de cada ítem.

III RESULTADOS Y DISCUSIÓN

El análisis de la transformación digital contable en Ecuador revela una división entre la adopción de infraestructura tecnológica de vanguardia y los mecanismos del control interno deberán ir acompañados con este proceso. Mientras el marco teórico subraya la importancia de una gobernanza integral basada en riesgos, la evidencia recolectada permite contrastar dichas premisas con la práctica profesional actual, los datos obtenidos mediante la encuesta aplicada a 138 profesionales de contabilidad y auditoría proporcionan una visión objetiva sobre el estado de la implementación de sistemas ERP, exponiendo vulnerabilidades críticas en la fase de diagnóstico previo y una marcada brecha en la capacitación especializada. Esta realidad coincide con lo expuesto por [17], quienes sostienen que la efectividad de los sistemas de información depende

básicamente de la alineación entre la arquitectura digital y el fortalecimiento de las competencias del talento humano para mitigar riesgos operativos.

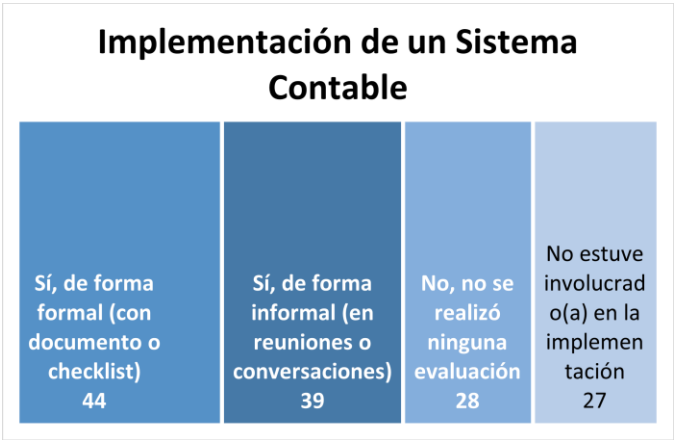
Gestión de Riesgos, diagnóstico preventivo Causa Raíz

La adopción tecnológica carece en su mayoría de un Gerente de proyecto, de un blindaje preventivo donde se confirma que la digitalización se percibe como un cambio técnico y no como proceso de gestión de riesgo financiero.

Nivel de formalidad en la evaluación de riesgos previa a la implementación de sistemas contables digitales.

Motivo	Cantidad	%
No estuve involucrado(a) en la implementación	27	20%
No, no se realizó ninguna evaluación	28	20%
Sí, de forma formal (con documento o checklist)	44	32%
Sí, de forma informal (en reuniones o conversaciones)	39	28%
Total	138	100%

FIG 1



Nota: Elaboración propia

Fig. 1 Nivel de formalidad en la evaluación de riesgos previa a la implementación de sistemas contables digitales.

La figura 1 revela una brecha crítica en la gestión preventiva de riesgos durante la digitalización contable en organizaciones ecuatorianas. Del total de 138 profesionales encuestados, apenas el 32% (44 casos) reporta haber participado en evaluaciones formales documentadas previo a la implementación. En contraste, el 28% (39 casos) indica que las evaluaciones fueron informales —limitadas a conversaciones sin metodología estructurada—, mientras que el 20% (28 casos)

confirma la ausencia total de diagnóstico preventivo. Un 20% adicional (27 casos) no estuvo involucrado en el proceso, lo que sugiere comunicación interna deficiente.

Estos hallazgos evidencian que casi la mitad de las implementaciones (50% sumando evaluaciones informales y ausencia de evaluación) carecen de un blindaje metodológico adecuado. Esta situación posiciona la digitalización como un cambio meramente técnico, desvinculado de la gestión estratégica de riesgos financieros que requieren los marcos regulatorios ecuatorianos (SRI, SEPS, Superintendencia de Compañías Valores y Seguros).

Limitar la digitalización al ámbito de TI, ignorando su impacto en el modelo de gestión y control, es un error crítico. La solidez técnica de una herramienta no garantiza el éxito si no existe una reingeniería de los procesos de supervisión, lo que eleva la probabilidad de errores tras la implementación.

Gestión Integral de la Autoeficacia y Capacitación Crítica como Blindaje Operativo ante la Falla Humana

El factor humano constituye la cadena más débil de la innovación de cambio de sistema y casi la mitad del personal recibió 5 días o menos de capacitación antes de usar sistemas críticos.

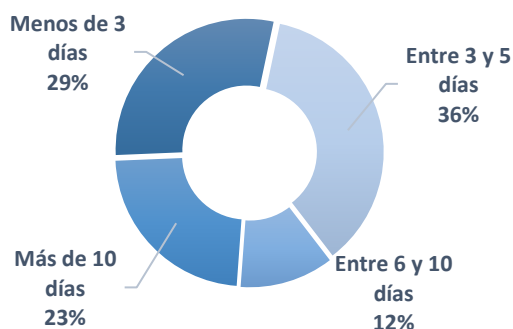
Duración de la capacitación recibida por el personal contable Durante la implementación del sistema digital.

FIG 2

Rango de días	Cantidad	%
Entre 3 y 5 días	50	36%
Entre 6 y 10 días	16	12%
Más de 10 días	32	23%
Menos de 3 días	40	29%
Total general	138	100%

Nota: Elaboración propia

Días de capacitación sobre sistemas contables



Nota: Elaboración propia

Fig. 2 Duración de la capacitación recibida por el personal contable durante la implementación.

La figura 2 expone la dimensión crítica del desarrollo de competencias digitales en el personal contable. Los datos revelan una distribución alarmante: el 29% (40 casos) recibió menos de 3 días de capacitación, mientras que el 36% (50 casos) tuvo entre 3 y 5 días. En conjunto, el 65% de la muestra fue capacitado en menos de una semana laboral.

Solo el 12% (16 casos) accedió a formación de 6 a 10 días, y únicamente el 23% (32 casos) superó los 10 días de entrenamiento. Esta insuficiencia formativa explica la baja percepción de autoeficacia detectada en dimensiones posteriores del estudio. Como sostienen Ocampo-Salazar, la tecnología sin desarrollo de competencias analíticas y operativas no solo es ineficaz para mitigar riesgos, sino que puede incrementarlos al generar una falsa sensación de control automatizado.

La brevedad educativa resulta insuficiente para el dominio de ecosistemas complejos como SAP, Fitbank u otro sistema recomendado, donde la falta de competencias analíticas y de control debilita el blindaje operativo del negocio provocando que incluso los sistemas mejor configurados fallen bajo una ejecución sub-capacitada que transforma al talento humano en el eslabón más vulnerable de la cadena de innovación.

Configuración, control interno y cumplimiento

La desconexión entre la capacidad de las herramientas y la ejecución del usuario genera riesgos de incumplimiento ante los entes de control.

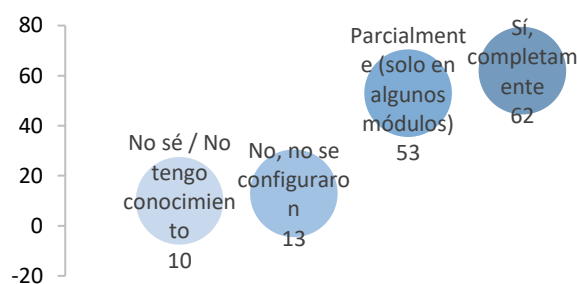
Relación entre la configuración de controles internos y la ocurrencia de hallazgos de auditoría o errores regulatorios

FIG 3

Motivo	Cantidad	%
No sé / No tengo conocimiento	10	7%
No, no se configuraron	13	9%
Parcialmente (solo en algunos módulos)	53	38%
Sí, completamente	62	45%
Total	138	100%

Nota: Elaboración propia

Configuración del Sistema Contable



Nota: Elaboración propia

Fig. 3 Relación entre la configuración de controles internos y la ocurrencia de hallazgos de auditoría.

La figura 3 ilustra una paradoja operativa significativa en la gestión de controles internos digitales. Mientras el 45% de los sistemas reporta configuraciones completas de segregación de funciones, aprobaciones digitales y límites de autorización, y el 38% cuenta con implementaciones parciales —sumando un 83% con algún nivel de control técnico—, la incidencia de hallazgos de auditoría y problemas regulatorios permanece elevada: el 32% reporta incidencias recurrentes y el 43% ocasionales.

Los datos revelan una paradoja que merece atención aunque la mayoría de los sistemas están bien configurados, los problemas de auditoría y regulatorio no desaparecen. La razón no está en el software — Están en las personas que la operan, ante las entidades de control SRI, SEPS, SCVS e IESS las falencias recurrentes se originan en el desconocimiento del

usuario, no en las limitaciones de la herramienta. Esto es una estrategia que genera riesgos legales y daña la confiabilidad de la información financiera. Un resumen de las deficiencias:

FIG 4

Dimensión	Problema identificado	Consecuencia
Riesgos	Falta de diagnóstico preventivo	Se implementa sin entender vulnerabilidades
Capacitación	Formación insuficiente (<5 días)	Personal no domina el sistema
Cumplimiento	Controles técnicos + mal uso	Persisten hallazgos pese a la tecnología

Nota: Elaboración Propia

La potencia de la herramienta se neutraliza ante el insuficiente dominio del usuario evidenciando que la causa raíz de las fallas no es de naturaleza técnica sino una carencia de capacitación humana que conecta directamente con la premisa de que la tecnología por sí sola es incapaz de mitigar riesgos operativos si el personal carece de las competencias analíticas necesarias para evitar que incluso los mejores controles configurados colapsen en la ejecución práctica.

Los hallazgos de este estudio confirman una tendencia preocupante en la digitalización contable ecuatoriana, la tecnología se adopta sin una arquitectura de control preventivo. A diferencia de lo observado en economías con marcos de gobernanza TI más maduros [18]; [19], donde la implementación de ERP se estructura desde marcos como COSO y COBIT, en el contexto local predomina un enfoque reactivo. En la validación de expertos la propuesta tuvo un coeficiente de W de Kendall de 0.81, lo cual demuestra un alto grado de concordancia entre los evaluadores con respecto de la pertinencia de la propuesta.

IV CONCLUSIONES

Los hallazgos de esta investigación revelan una debilidad estructural en la gestión de proyectos de innovación tecnológica en el sector contable ecuatoriano, caracterizada por una gestión preventiva deficiente y la ausencia de marcos de gobernanza estratégica como COSO o COBIT. A pesar de que el 83.3% de las organizaciones dispone de sistemas con configuraciones técnicas de control, solo el 37% ejecutó evaluaciones formales de riesgo previas a la implementación, lo que reduce la transformación digital a un plano meramente operativo y desprovisto de visión prospectiva. Esta desconexión entre la

infraestructura técnica y la planificación estratégica explica por qué las incidencias reportadas ante entes reguladores como el SRI, SEPS, SCVS e IESS —que afectan al 75% de la muestra— no constituyen eventos aislados, sino síntomas sistémicos de una implementación desvinculada de los protocolos de control interno y cumplimiento normativo exigidos en el país.

Asimismo, se identifica una brecha crítica en el desarrollo del capital humano como el principal inhibidor de la eficacia de los sistemas ERP, dado que el 65% de los profesionales recibió una formación técnica inferior a cinco días. Esta limitación temporal configura una paradoja tecnológica: la sofisticación de los controles digitales (segregación de funciones y firmas electrónicas) es neutralizada por la impericia del usuario, perpetuando un ciclo de errores operativos y hallazgos de auditoría recurrentes. En conclusión, el éxito de la digitalización contable en Ecuador no depende exclusivamente de la adquisición de software, sino de la adopción de un modelo de gestión integral que priorice la capacitación especializada y la auditoría preventiva como pilares para garantizar la integridad financiera y la transparencia institucional.

V. RECOMENDACIÓN

Por lo expuesto se recomienda la designación estratégica de un Gerente de Proyecto (Project Manager) con un perfil híbrido que integre competencias en gestión de tecnologías de información y marcos de gestión de riesgos financieros. Este rol debe actuar como el eje articulador de equipos multidisciplinarios —contabilidad, auditoría, legal y TI—, asegurando que la arquitectura del sistema ERP responda a las necesidades de control interno y cumplimiento normativo. Al establecer una línea de reporte directo hacia la Alta Dirección, se garantiza que la implementación trascienda el plano técnico para convertirse en un proceso de gobernanza institucional, mitigando proactivamente las vulnerabilidades operativas y asegurando la alineación de la innovación tecnológica con los objetivos estratégicos de la organización.

Establecer como imperativo metodológico la implementación de una matriz de diagnóstico integral previa a la adopción tecnológica, la cual debe converger los cinco componentes del marco COSO con los dominios de gobernanza de COBIT como, por ejemplo:

Cuestionario de Control Interno

Dimensión Componente (COSO/COBIT)	Pregunta clave / Control mínimo	SI	NO	N/A	Responsable
Entorno de Control (COSO – Entorno de Control)	¿Existe compromiso de la alta dirección con la integridad y ética en la implementación del ERP?				Gerencia General
Evaluación de Riesgos (COSO – Evaluación de Riesgos)	¿Se identificaron riesgos específicos relacionados con: pérdida de datos, errores en conciliaciones, accesos no autorizados?				Equipo de Proyecto + Auditoría
Actividades de Control (COSO – Actividades de Control)	¿Se diseñaron controles digitales para: segregación de funciones, aprobaciones electrónicas, límites de gasto?				TI + Contabilidad
Información y Comunicación (COSO – Información)	¿El sistema garantiza trazabilidad completa de transacciones financieras según NIIF?				Contabilidad + TI
Monitoreo (COSO – Monitoreo)	¿Se establecerá un plan de revisión post-implementación (primeros 6 meses)?				Auditoría Interna
Gobernanza de TI (COBIT – EDM01 (Asegurar la gobernanza))	¿La implementación del ERP está alineada con los objetivos estratégicos de la organización?				Comité de TI
Gestión de Riesgos TI (COBIT – APO12 (Gestión de riesgos))	¿Se evaluaron riesgos cibernéticos, de disponibilidad y de integridad de la información financiera?				Seguridad TI
Cumplimiento Normativo (COBIT – MEA03 (Monitoreo de cumplimiento))	¿El sistema cumple con los requisitos del SRI, SEPS, IESS y CGE (si aplica)?				Legal + Contabilidad

Este instrumento técnico debe ejecutarse como fase previa a la implementación para identificar vulnerabilidades en el ambiente de control y la valoración de riesgos financieros.

Establece como requisito estratégico la implementación de un programa de capacitación técnica de al menos 40 horas, estructurado de forma escalonada para mitigar la brecha de competencias identificada en el estudio. Este plan debe ejecutarse en tres etapas críticas: una fase de pre-implementación (16 horas) enfocada en la arquitectura de controles internos; una fase de puesta en marcha (16 horas) basada en práctica supervisada con escenarios transaccionales reales; y una fase de consolidación (8 horas trimestrales) destinada a la actualización normativa y operativa durante el primer año. Esta metodología de formación continua garantiza que el capital humano trascienda la operatividad básica hacia un dominio experto de los controles automáticos, reduciendo significativamente la incidencia de hallazgos de auditoría y errores financieros.

Realizar un protocolo de monitoreo continuo mediante la definición de Indicadores Clave de Riesgo (KRI) mensuales, orientados a la detección temprana de anomalías operativas. Este sistema de supervisión debe priorizar métricas críticas como el porcentaje de errores en validaciones transaccionales, la frecuencia de accesos no autorizados y los tiempos de conciliación bancaria, alineando la operatividad del ERP con las exigencias de transparencia de los entes reguladores (SRI, SEPS y Superintendencia de Compañías Valores y Seguros). La implementación de estos indicadores transforma la auditoría en un proceso dinámico y preventivo, garantizando la integridad de la información financiera y mitigando el riesgo de sanciones legales por inconsistencias sistémicas.

Se propone el desarrollo de una Guía Técnica de Implementación de Sistemas Contables Digitales, concebida como un marco regulatorio de requisitos mínimos para las organizaciones bajo supervisión. Este instrumento debe estandarizar los protocolos obligatorios de control interno preventivo, los umbrales mínimos de capacitación técnica y los estándares de documentación de sistemas necesarios para garantizar la integridad de la data financiera. La adopción de esta guía técnica permitiría uniformar la calidad de la gobernanza digital en el sector, reduciendo la asimetría de controles detectada en este estudio y facilitando los procesos de fiscalización y auditoría externa mediante una estructura de cumplimiento predefinida y auditable.

Se recomienda la reingeniería de los protocolos de fiscalización para integrar la auditoría de activos intangibles y gobernanza digital. Este proceso debe exigir de forma mandataria la documentación de evaluación previa de riesgos,

la evidencia certificada de capacitación técnica del personal y la validación de la configuración de controles digitales (segregación de funciones y trazabilidad). Al incorporar estos requisitos en las auditorías externas, se garantiza que el cumplimiento normativo no sea solo declarativo, sino que esté sustentado en una infraestructura de control robusta que minimice la opacidad financiera y el riesgo sistémico en el ecosistema contable digital.

VI. AGRADECIMIENTO Y RECONOCIMIENTO

Los autores agradecen a la Universidad Bolivariana del Ecuador por el apoyo brindado en el desarrollo de esta investigación, así como a los 138 profesionales de contabilidad y auditoría que participaron voluntariamente en la encuesta. Se reconoce también la valiosa contribución de los expertos evaluadores del instrumento por sus observaciones técnicas.

REFERENCES

- [1] Ministerio de Telecomunicaciones y de la Sociedad de la Información, Agenda de Transformación Digital del Ecuador 2022-2025, Ecuador, 2025.
- [2] R. I. Ortega, Contabilidad en la era digital: Análisis cómo las tecnologías están transformando los procesos contables en las Pymes de Ecuador, LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, vol. 6, no. 1, pp. 2904-2915, 2025.
- [3] E. G. Feijoo, Transformación digital en la contabilidad de las pequeñas y medianas empresas en la provincia de El Oro, Ecuador, Revista Venezolana de Gerencia, vol. 29, no. 108, 2024.
- [4] M. X. Álava, Contribución de la auditoría interna para alcanzar una gestión eficaz, LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, vol. 4, no. 4, pp. 1217-1227, 2023.
- [5] SENESCYT, Proyecto de Inversión para el Desarrollo de Actividades de Ciencia, Tecnología e Innovación, 2022.
- [6] C. G. Mendoza, El control interno y su influencia en la gestión administrativa de los sectores públicos, Spirales Revista Multidisciplinaria de Investigación, vol. 2, no. 19, 2018.
- [7] Contraloría General del Estado, Normas de control interno de la Contraloría General del Estado, Registro Oficial Suplemento 87, Ecuador, 2014.
- [8] A. López, El control interno en el sector público ecuatoriano, Cofin Habana, vol. 12, no. 2, 2018.
- [9] A. M. Ocampo, Efectos de la transformación digital en el sector contable y financiero en Ecuador, Ciencia y Educación, vol. 4, no. 11, pp. 42-52, 2023.
- [10] L. Zamora, Control interno y gestión financiera de las PyMEs de servicios del Cantón Manta, Horizon Nexus Journal, vol. 3, no. 2, 2025.
- [11] SMS Ecuador, Implementación de las NIIF y NIIF PYMES en Ecuador, 2025. [En línea]. Disponible en: <https://smsecuador.ec/implementacion-de-las-niif-y-niif-pymes-en-ecuador/>.
- [12] J. D.-M. Gordillo-Mejía, Adopción de las NIIF en empresas emergentes: desafíos y estrategias de implementación, Revista Metropolitana de Ciencias Aplicadas, vol. 7, no. S2, pp. 99-107, 2024.
- [13] R. D.-C. Martínez-Punina, NIIF para pequeñas y medianas empresas y su implementación en Ecuador, Fundación Koinonia, vol. 10, no. 1, 2025.
- [14] PwC Ecuador, Auditoría y gobierno corporativo, 2023. [En línea]. Disponible en: <https://www.pwc.ec/es/servicios/otros-servicios.html>.
- [15] M. S. Torres, Auditoría Integral, Research Gate, 2022.
- [16] Secureframe, Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), 2025. [En línea]. Disponible en: <https://secureframe.com/es-es/frameworks-glossary/cobit>.
- [17] C. A. Ocampo-Salazar et al., Transformación digital en la contabilidad: Una revisión sistemática de la literatura sobre las competencias del contador, Revista CEA, vol. 10, no. 22, p. e2654, 2024.
- [18] A. A.-S. Alshammari, Information technology governance and enterprise resource planning system adoption: The mediating role of internal control systems, International Journal of Accounting Information Systems, vol. 46, 100570, 2022.
- [19] B. L. Handoko, The impact of IT governance on the quality of accounting information systems: The case of Indonesian listed companies, Journal of Theoretical and Applied Information Technology, vol. 101, no. 5, pp. 1824-1835, 2023.

ANEXOS

ANEXO DE ENCUESTAS A PROFESIONALES

Como complemento al análisis documental, se aplicó un breve sondeo probabilístico descriptivo a 138 profesionales contables en Ecuador a nivel nacional, cuyos resultados preliminares refuerzan el hallazgo de una brecha entre la adopción tecnológica y la preparación del talento humano.

Implementación de sistemas contables digitales en Ecuador: percepción de profesionales contables

Este breve cuestionario busca recoger su experiencia sobre la implementación de sistemas contables digitales (como SAP, Fitbank, Eonx, etc.) en organizaciones del Ecuador. Sus respuestas serán anónimas y de gran valor para una investigación académica en curso.

Por favor, responda según su vivencia laboral. ¡Gracias por su colaboración!

Cuando su organización implementó un sistema contable digital (como SAP, Fitbank, Econx, etc.), ¿se realizó una evaluación previa de riesgos financieros o controles internos? (Selecciona una opción)

- Sí, de forma formal (con documento o checklist)
- Sí, de forma informal (en reuniones o conversaciones)
- No, no se realizó ninguna evaluación
- No estuve involucrado(a) en la implementación

¿Cuántos días de capacitación recibió el personal contable o administrativo antes o durante la implementación del sistema? (Escribe un número aproximado)

- Menos de 3 días
- Entre 3 y 5 días
- Entre 6 y 10 días
- Más de 10 días
- No hubo capacitación

¿Se configuraron en el sistema controles como aprobaciones digitales, segregación de funciones o límites de autorización? (Selecciona una opción)

- Sí, completamente
- Parcialmente (solo en algunos módulos)
- No, no se configuraron
- No sé / No tengo conocimiento

¿Ha observado errores, hallazgos de auditoría o problemas regulatorios (ante SRI, SEPS, IEES, etc.) relacionados con el mal uso o desconocimiento del sistema contable? (Selecciona una opción)

- Sí, en varias ocasiones
- Sí, en alguna ocasión
- No, nunca
- No estoy en condiciones de saberlo

En su opinión, ¿la capacitación recibida fue suficiente para garantizar un uso seguro y eficaz del sistema? (Selecciona una opción)

- Sí, completamente suficiente
- Parcialmente suficiente
- No, fue insuficiente
- No hubo capacitación