HORIZON NEXUS JOURNAL
ISSN: 3073-1275

DOSO EDITORIAL CIENTÍFICA

Articulo

Control interno informático en los sistemas contables: Análisis del ERP Odoo community

Computational internal control in accounting systems: Analysis of The Odoo Community ERP

Rudy Ivonne Ortega Cabrera [1]*, Aida Maribel Palma León [2], Martha Matilde Sandoval Cují [3], Jaritza Xiomara Ortega Méndez [4]

[1] Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo; https://orcid.org/0000-0001-7518-6688

[2] Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo; https://orcid.org/0000-0003-3982-1132, aplama@uteq.edu.ec

[3] Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo; https://orcid.org/0000-0002-5182-3280; msaldoval@uteq.edu.ec

[4] Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo; https://orcid.org/0000-0002-8268-1617, jortegam4@uteq.edu.ec

* Correspondencia: rortega@uteq.edu.ec

https://doi.org/10.70881/hnj/v4/n1/105

Cita: Ortega Cabrera, R. I., Palma León, A. M., Sandoval Cují, M. M., & Ortega Méndez, J. X. (2026). Control interno informático en los sistemas contables: Análisis del ERP Odoo community. *Horizon Nexus Journal*, *4*(1), 138-154. https://doi.org/10.70881/hnj/v4/n1/105

Recibido: 04/02/2026
Revisado: 01/03/2026
Aceptado: 03/03/2026
Publicado: 06/03/2026

Resumen: La presente investigación analiza el control interno informático en los sistemas contables mediante el estudio del ERP Odoo Community, considerando los principios del Marco Integrado de Control Interno COSO y los dominios del Marco de Gobernanza y Gestión de Tecnologías de la Información COBIT 2019, en un contexto de creciente digitalización de los procesos contables. El estudio adopta un enfoque cuantitativo, con un diseño descriptivo, no experimental y de corte transversal, utilizando la encuesta como técnica de recolección de datos aplicada a 60 profesionales del área contable que emplean Odoo Community como sistema contable, a través de un cuestionario estructurado con escala de Likert de cinco niveles. Los resultados evidencian que más del 60 % de los encuestados percibe positivamente la definición de roles y permisos de usuario; sin embargo, aproximadamente el 45 % manifiesta percepciones neutrales o negativas respecto a la identificación de riesgos informáticos y menos del 50 % reconoce la realización de evaluaciones y revisiones periódicas del sistema. En conclusión, aunque Odoo Community dispone de funcionalidades que permiten implementar controles internos informáticos, estos no se encuentran plenamente fortalecidos ni alineados de manera integral con los marcos COSO y COBIT 2019, lo que evidencia la necesidad de fortalecer la gestión de riesgos, la supervisión continua y la seguridad de la información contable.

Palabras clave: Control interno, auditoria de sistemas, ERP, Riesgo.

Abstract: This research analyzes IT internal control in accounting systems through the study of the Odoo Community ERP, considering the principles of the COSO Internal Control Framework and the domains of the COBIT 2019 Governance and Management of IT Framework, in a context of increasing digitalization of accounting processes. The study adopts a quantitative approach, with a descriptive, non-experimental, and cross-sectional design, using a survey as the data collection technique. The instrument, structured

on a five-point Likert scale, is applied to 60 accounting professionals who use Odoo Community as their accounting system, evaluating dimensions related to user roles and permissions, identification of IT risks, detection of unauthorized access, reliability of accounting information, and periodic system reviews. The results show that more than 60% of respondents positively perceive the definition of user roles and access controls; however, approximately 45% report neutral or negative perceptions regarding IT risk identification, and less than 50% acknowledge the performance of periodic evaluations and reviews. These findings indicate weaknesses in risk management and monitoring processes. The study concludes that, although Odoo Community provides functionalities that support IT internal control, these controls are not fully strengthened nor comprehensively aligned with COSO and COBIT 2019, highlighting the need to enhance risk management, continuous monitoring, and information security to ensure the reliability of accounting information.

Keywords: Internal control; Accounting systems; ERP; Risk.

1. Introducción

Las tecnologías de la información han transformado el ámbito organizacional, impulsando la competitividad, la eficiencia operativa y el diseño de reportes gerenciales para la toma de decisiones. En el campo contable, su incorporación resulta esencial para optimizar procesos financieros, reducir errores y agilizar registros diarios(Salgado Reyes et al., 2024).

En la actualidad, las tecnologías de la información desempeñan un papel determinante en la gestión organizacional, especialmente en el ámbito contable, donde los sistemas informáticos se convierten en el eje central para el procesamiento, almacenamiento y presentación de la información financiera (Laudon & Laudon, 2022). Los sistemas de planificación de recursos empresariales (ERP) permiten integrar procesos contables, financieros y administrativos en una única plataforma, contribuyendo a mejorar la eficiencia operativa y la calidad de la información para la toma de decisiones (Govea Souza, 2021; Noesis, 2025). No obstante, esta integración tecnológica incrementa la exposición a riesgos informáticos, como accesos no autorizados, pérdida o manipulación de datos, lo que hace imprescindible el fortalecimiento del control interno informático en los sistemas contables (Romney & Steinbart, 2021; ISACA, 2019).

El control interno se concibe como un conjunto de políticas y procedimientos orientados a salvaguardar los activos, garantizar la confiabilidad de la información financiera y asegurar el cumplimiento normativo (COSO, 2017). Diversas investigaciones sostienen que la efectividad del control interno depende, en gran medida, del adecuado diseño y uso de los sistemas de información contable, especialmente en entornos digitalizados (Vaca Benalcázar, 2016; Huamán Heredia, 2022). En este sentido, el control interno informático surge como una respuesta a los desafíos tecnológicos actuales,

debido a la creciente dependencia de los sistemas de información contable, enfocándose en la protección de los datos, la seguridad de los sistemas y la integridad de los procesos contables automatizados (ISACA, 2019).

Desde una perspectiva macro, la literatura evidencia que la implementación de sistemas ERP impacta positivamente en la gestión empresarial al integrar información contable y operativa, reducir errores y optimizar los procesos administrativos (Vallejo Ballesteros & Aguilar Wilca, 2024; Utopía y Praxis Latinoamericana, 2021a). Sin embargo, también se advierte que la ausencia de controles internos adecuados en entornos ERP puede generar debilidades relacionadas con accesos no autorizados, deficiencias en la segregación de funciones y riesgos en la confiabilidad de la información contable (Zhang, He & Tao, 2014).

A nivel meso, estudios especializados destacan que el control interno en ambientes ERP requiere la implementación de controles automáticos, auditorías de acceso, perfiles de usuario y mecanismos de validación de la información financiera, los cuales permiten reducir los riesgos inherentes a los sistemas integrados (Chang, 2013; Yao & Yang, 2014). Asimismo, se ha demostrado que el control interno actúa como un factor mediador entre los sistemas de información contable y los resultados financieros, contribuyendo a mejorar el desempeño organizacional y la calidad de la información financiera (Alcántara Hernández et al., 2023; Utopía y Praxis Latinoamericana, 2021b).

En el contexto latinoamericano, diversas investigaciones evidencian que la digitalización de los procesos contables, como la facturación electrónica y la automatización financiera, exige un control interno informático sólido que garantice la transparencia, la confiabilidad y el cumplimiento normativo (Rojas Quispe et al., 2026; Huamán Heredia, 2022). Asimismo, se reconoce que las pequeñas y medianas empresas enfrentan mayores desafíos en la implementación de controles internos informáticos, lo que incrementa la necesidad de evaluar soluciones ERP accesibles y flexibles (Vallejo Ballesteros & Aguilar Wilca, 2024).

Desde una perspectiva micro, el ERP Odoo Community se presenta como una solución de código abierto ampliamente adoptada por organizaciones que buscan integrar sus procesos contables y administrativos. Investigaciones recientes analizan su implementación y destacan su capacidad para automatizar procesos contables y mejorar la trazabilidad de la información; no obstante, también señalan la necesidad de evaluar sus mecanismos de control interno informático para asegurar un uso eficiente y seguro del sistema (Utami & Kharisma, 2023; Vadsya, Witjaksono & Puspitasari, 2023). En este sentido, resulta relevante analizar cómo se aplican los controles internos informáticos en

los módulos contables de Odoo Community y su impacto en la gestión de la información financiera.

El problema científico que fundamenta esta investigación radica en la limitada evidencia empírica sobre la efectividad del control interno informático en los sistemas contables basados en el ERP Odoo Community, especialmente desde la percepción de los usuarios que interactúan directamente con el sistema. La justificación del estudio se sustenta en la creciente adopción de este ERP en organizaciones que requieren sistemas contables confiables y alineados con principios de control interno y gestión de riesgos tecnológicos (Govea Souza, 2021; Noesis, 2025).

En cuanto a la metodología, la investigación adopta un enfoque cuantitativo, utilizando la técnica de la encuesta como instrumento principal para la recolección de datos. Las encuestas se aplican a usuarios del sistema contable que operan el ERP Odoo Community, con el propósito de analizar su percepción sobre los mecanismos de control interno informático, la seguridad de la información, la confiabilidad de los registros contables y la eficiencia de los procesos automatizados, siguiendo enfoques metodológicos empleados en estudios previos sobre sistemas de información contable y control interno (Huamán Heredia, 2022; Rojas Quispe et al., 2026).

En consecuencia, el objetivo principal de la presente investigación es analizar el control interno informático en los sistemas contables mediante el estudio del ERP Odoo Community, a partir de la aplicación de encuestas a los usuarios del sistema, con el fin de identificar fortalezas, debilidades y oportunidades de mejora que contribuyan a la confiabilidad y eficiencia de la información contable.

2. Materiales y Métodos

Enfoque de la investigación

La presente investigación se desarrolla bajo un enfoque cuantitativo, debido a que se fundamenta en la recolección y análisis de datos numéricos con el propósito de evaluar el nivel de control interno informático en el sistema contable Odoo Community. Este enfoque permite medir la percepción de los usuarios y analizar los resultados mediante procedimientos estadísticos, facilitando la obtención de conclusiones objetivas en relación con el fenómeno estudiado.

Tipo y diseño de la investigación.

El estudio es de tipo descriptivo, ya que tiene como finalidad caracterizar el nivel de control interno informático existente en el sistema contable, sin manipular las variables de estudio. Asimismo, se adopta un diseño no experimental, debido a que los hechos se observan en su contexto natural sin intervención del investigador. Además, el diseño es transversal, puesto que la recolección de datos se realiza en un único momento del tiempo.

Población y muestra

La población está conformada por profesionales del área contable que utilizan el sistema Odoo Community como herramienta para el registro y gestión de la información financiera en su actividad laboral. La muestra está constituida por 60 profesionales del área contable, seleccionados mediante un muestreo no probabilístico por conveniencia. Este tipo de muestreo se emplea debido a la accesibilidad de los participantes, su experiencia directa en el uso del sistema y su disponibilidad para participar en el estudio.

Técnica e instrumento de recolección de datos

La técnica utilizada para la recolección de datos es la encuesta, por ser un método adecuado para obtener información directamente de los usuarios del sistema.
El instrumento aplicado es un cuestionario estructurado, diseñado con base en los principios establecidos en el Marco Integrado de Control Interno COSO (2017) y en los dominios del Marco de Gobernanza y Gestión de Tecnologías de la Información COBIT 2019. El cuestionario está compuesto por ítems organizados en dimensiones relacionadas con roles y permisos de usuario, identificación de riesgos informáticos, detección de accesos no autorizados, confiabilidad de la información contable y evaluaciones periódicas del sistema.

Escala de medición

Para la medición de las respuestas se utiliza una escala de Likert de cinco niveles, donde el valor 1 corresponde a “Totalmente en desacuerdo”, el valor 2 a “En desacuerdo”, el valor 3 a “Ni de acuerdo ni en desacuerdo”, el valor 4 a “De acuerdo” y el valor 5 a “Totalmente de acuerdo”. Esta escala permite cuantificar la percepción de los encuestados y facilita el análisis estadístico de los datos.

Procesamiento y análisis de datos

El procesamiento de la información se realiza mediante estadística descriptiva. Para el análisis se emplean frecuencias absolutas y relativas, expresadas en porcentajes, lo que permite interpretar el comportamiento de las respuestas en cada una de las dimensiones evaluadas.
Los resultados se presentan mediante tablas y figuras, con el propósito de facilitar la visualización e interpretación del nivel de control interno informático existente en el sistema contable Odoo Community.

3. Resultados

Los resultados obtenidos mediante la aplicación de una encuesta estructurada en escala de Likert a 60 profesionales del área contable permitieron evaluar la percepción del nivel de control interno informático en el sistema contable Odoo

Community, considerando los principios del marco COSO (2017) y los dominios de COBIT 2019.

Escala de valoración Likert

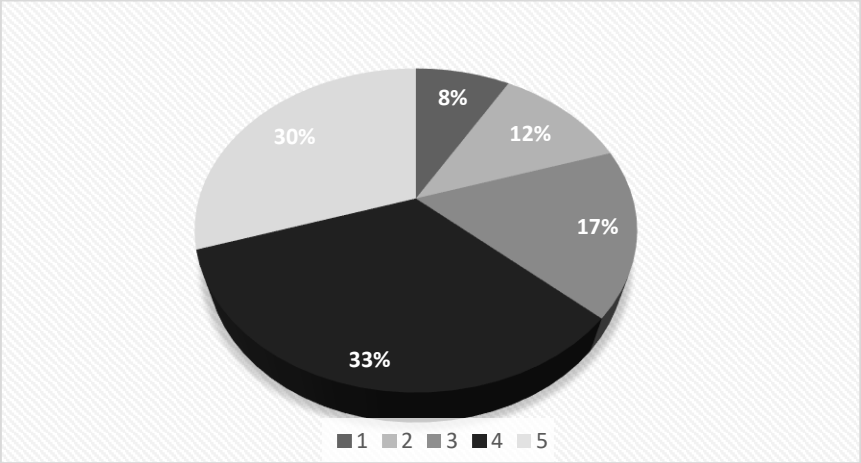
- Totalmente en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

Roles y permisos definidos

La Figura 1 presenta los resultados relacionados con la definición de roles y permisos de usuario en el sistema contable Odoo Community. Se observa que la mayoría de los encuestados se concentra en las categorías De acuerdo y Totalmente de acuerdo, lo que evidencia que el sistema dispone de mecanismos para la asignación de accesos conforme a las funciones del usuario. Estos resultados reflejan la existencia de controles orientados a restringir el acceso a la información contable.

Sin embargo, también se registran respuestas en las categorías Ni de acuerdo ni en desacuerdo y En desacuerdo, lo que muestra que estos controles no se aplican de manera homogénea en todos los casos. Esta situación se relaciona con el componente ambiente de control del COSO (2017) y con el dominio DSS05 Gestión de la seguridad de los servicios de COBIT 2019.

Figura 1
Roles y permisos definidos



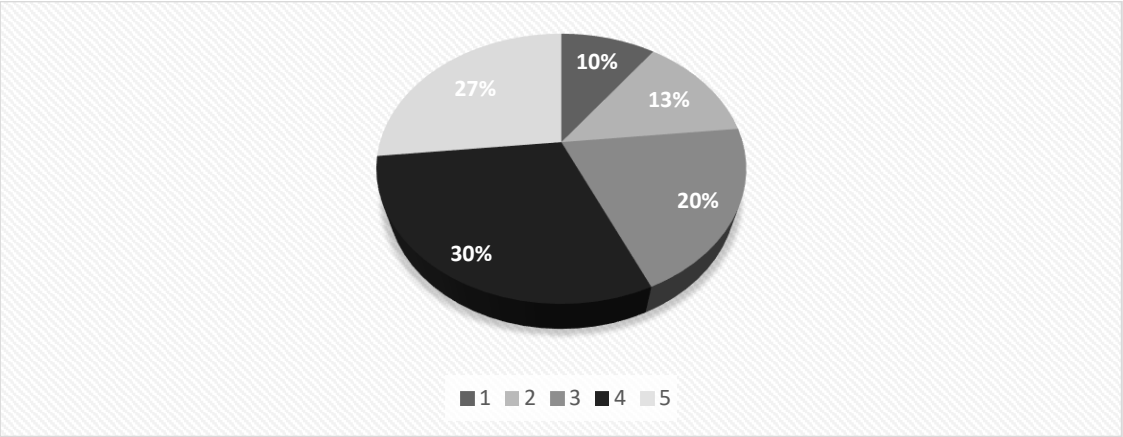
Identificación de riesgos informáticos

La Figura 2 muestra los resultados relacionados con la identificación de riesgos informáticos en el sistema contable. Se observa que una parte importante de los encuestados manifiesta estar de acuerdo con la existencia de mecanismos de identificación de riesgos. No obstante, también se evidencia la presencia de respuestas en niveles neutral y en desacuerdo.

Estos resultados indican que la identificación de riesgos informáticos no se realiza de forma consistente en todos los casos, lo que limita la capacidad preventiva del sistema. Este aspecto se vincula con el componente evaluación de riesgos del COSO (2017) y con el proceso APO12 Gestión de riesgos de COBIT 2019.

Figura 2

Identificación de riesgos informáticos



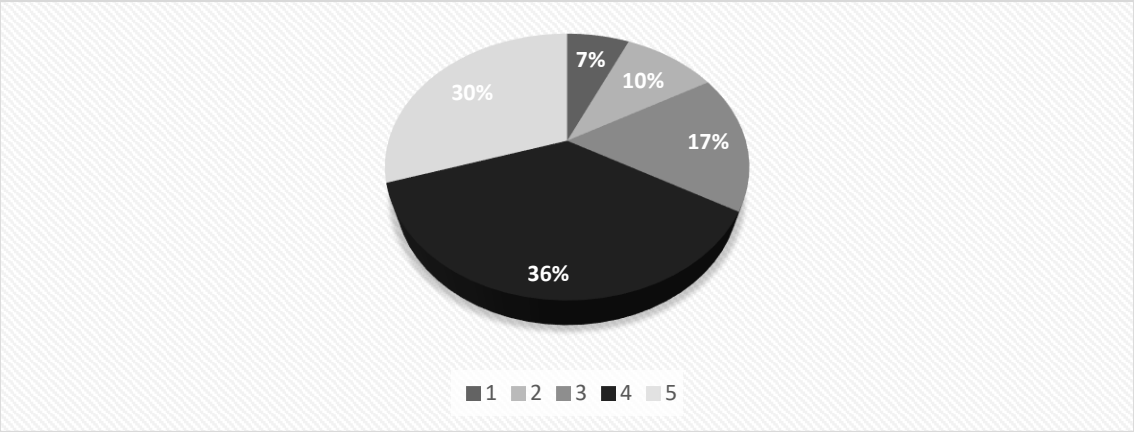
Detección de accesos no autorizados

La Figura 3 presenta los resultados relacionados con la detección de accesos no autorizados. Se observa que una proporción relevante de los encuestados manifiesta una percepción favorable sobre este aspecto. Sin embargo, también se registran respuestas en niveles neutral y en desacuerdo.

Estos resultados muestran que los mecanismos de monitoreo y control de accesos no presentan el mismo nivel de efectividad en todos los casos, lo que puede afectar la seguridad de la información contable. Este resultado se relaciona con el componente actividades de control del COSO (2017) y con el dominio DSS06 Gestión de controles de procesos de negocio de COBIT 2019.

Figura 3

Detección de accesos no autorizados



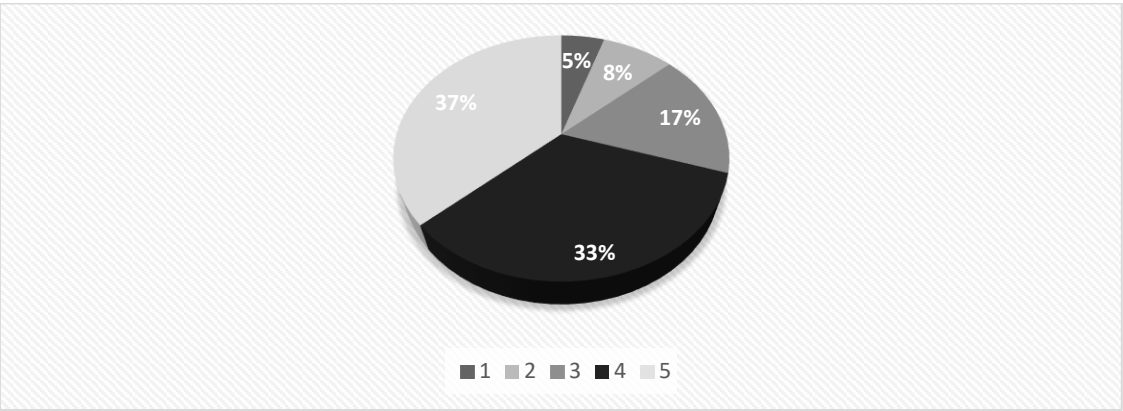
Confiabilidad de la información contable

La Figura 4 muestra los resultados relacionados con la confiabilidad de la información contable generada por el sistema. Se observa que la mayoría de los encuestados manifiesta estar de acuerdo y totalmente de acuerdo, lo que evidencia una percepción favorable respecto a la calidad de la información generada.

No obstante, la presencia de respuestas en niveles neutral y en desacuerdo refleja que la confiabilidad de la información puede verse influenciada por la aplicación de los controles informáticos. Este resultado se relaciona con el componente información y comunicación del COSO (2017).

Figura 4

Confiabilidad de la información contable



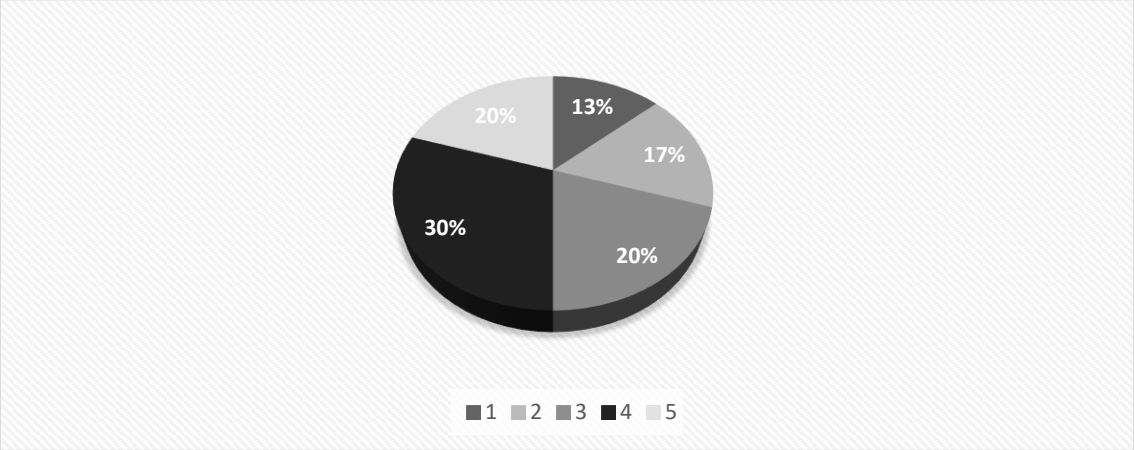
Evaluaciones y revisiones periódicas

La Figura 5 presenta los resultados relacionados con la ejecución de evaluaciones y revisiones periódicas del sistema. Se observa una menor concentración de respuestas en los niveles De acuerdo y Totalmente de acuerdo en comparación con las demás dimensiones.

Estos resultados evidencian la existencia de limitaciones en la supervisión continua del control interno informático, lo que reduce la capacidad de detectar oportunamente posibles deficiencias en el sistema. Este aspecto se relaciona con el componente supervisión del COSO (2017) y con el dominio MEA01 Monitoreo del desempeño y conformidad de COBIT 2019.

Figura 5

Evaluaciones y revisiones periódicas



Comparación entre COBIT, ISO/IEC 27001 e inteligencia artificial

La Tabla 1 presenta una comparación entre los marcos COBIT, ISO/IEC 27001 y la inteligencia artificial, considerando su enfoque, gestión de riesgos y contribución al proceso de auditoría. Se observa que COBIT se orienta a la gobernanza y gestión de las tecnologías de la información, mientras que ISO/IEC 27001 se enfoca en la gestión de la seguridad de la información mediante la implementación de controles específicos. Por su parte, la inteligencia artificial contribuye mediante la automatización de procesos, el análisis predictivo y la detección de anomalías en tiempo real.

Estos enfoques no son excluyentes, sino complementarios, debido a que COBIT proporciona la estructura de gobernanza, ISO/IEC 27001 establece los controles de seguridad, y la inteligencia artificial fortalece la eficiencia de los controles mediante el monitoreo continuo. Esta integración contribuye a mejorar la capacidad de las organizaciones para prevenir, detectar y responder a riesgos informáticos, fortaleciendo el control interno informático y el proceso de auditoría.

Tabla 1

Comparación entre COBIT, ISO/IEC 27001 e inteligencia artificial

Aspecto	COBIT	ISO/IEC 27001	Inteligencia Artificial

Enfoque	Gobernanza y gestión de TI	Gestión de seguridad de la información	Automatización y análisis predictivo
Riesgos	Riesgos tecnológicos	Riesgos de seguridad de la información	Detección de anomalías en tiempo real
Auditoría	Evaluación de madurez y control	Cumplimiento normativo	Auditoría continua

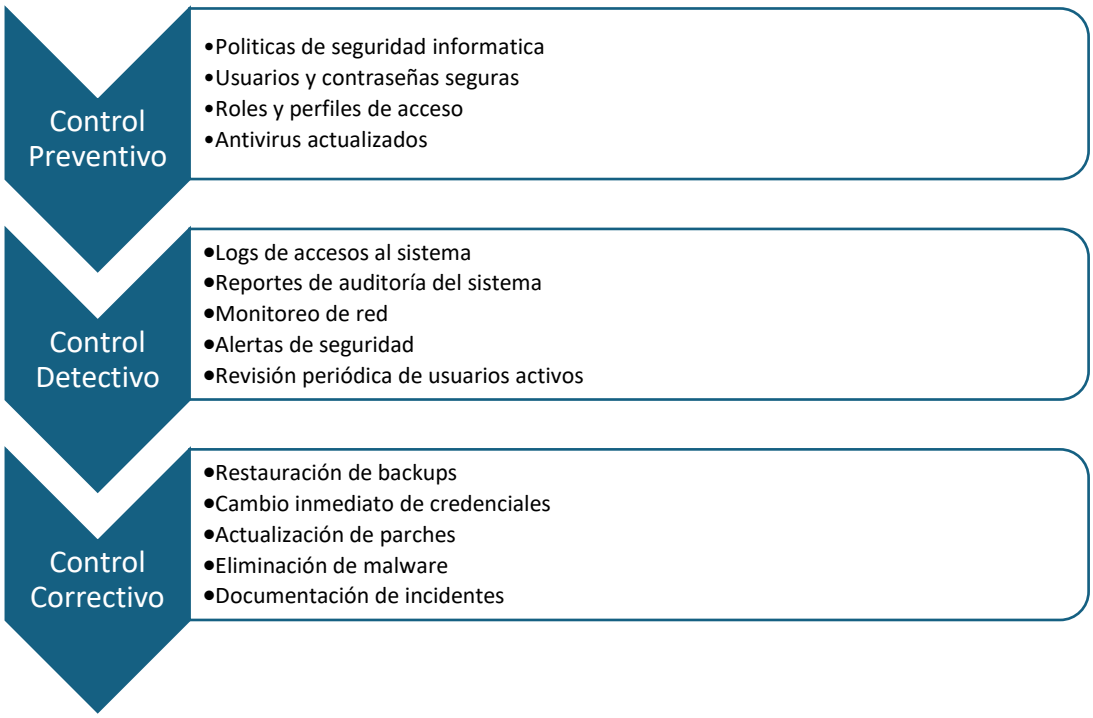
Controles internos informáticos aplicables al sistema

La Tabla 2 presenta los principales controles internos informáticos aplicables al sistema contable Odoo Community. Estos controles se relacionan con la seguridad lógica, la integridad de la información, la disponibilidad del sistema y la trazabilidad de las operaciones.

La implementación de estos controles permite fortalecer la protección de la información contable, reducir la probabilidad de ocurrencia de riesgos informáticos y mejorar la confiabilidad de los reportes financieros. Asimismo, contribuyen a garantizar el adecuado funcionamiento del sistema y el cumplimiento de los objetivos del control interno informático.

Tabla 2

Controles internos informáticos



Identificación de riesgos informáticos

La Tabla 3 muestra los principales riesgos informáticos a los que se encuentran expuestos los sistemas contables informatizados, incluyendo el acceso no autorizado, la pérdida de información, la alteración de datos, la indisponibilidad del sistema, la presencia de software malicioso y la falta de respaldos.

Estos riesgos representan amenazas significativas para la seguridad, integridad y disponibilidad de la información contable. En particular, el acceso no autorizado, la pérdida de información y la alteración de datos pueden afectar la confiabilidad de los reportes financieros y la toma de decisiones. Por esta razón, es necesario implementar controles preventivos y correctivos que permitan reducir la exposición al riesgo y garantizar la continuidad operativa del sistema.

Tabla 3

Identificación de riesgos informáticos

Riesgo	Descripción
Acceso no autorizado	Uso indebido de sistemas o información
Pérdida de información	Fallas, virus o errores humanos
Alteración de datos	Manipulación no autorizada
Indisponibilidad	Caídas del sistema o red
Malware	Virus, ransomware, spyware
Falta de respaldo	No recuperación de información

Hallazgos de riesgos informáticos en el sistema contable Odoo Community

Gestión de usuarios

Se identificó como principal riesgo el acceso no autorizado al sistema contable, originado por una inadecuada definición de roles y el uso de cuentas genéricas. Esta situación incrementa la probabilidad de manipulación de la información contable y afecta la seguridad del sistema. El nivel de riesgo determinado es alto, debido a la probabilidad y el impacto asociados. Este hallazgo evidencia la necesidad de implementar controles orientados a la segregación de funciones y la asignación de perfiles de usuario según responsabilidades, en concordancia con el componente ambiente de control del marco Committee of Sponsoring Organizations of the Treadway Commission y el proceso DSS05 del marco ISACA.

Proceso contable

Se evidenció el riesgo de modificación indebida de asientos contables, debido a la ausencia de registros de auditoría y mecanismos de trazabilidad. Esta condición afecta la integridad y confiabilidad de la información financiera,

generando un nivel de riesgo alto. La inexistencia de controles automatizados limita la capacidad de identificar cambios realizados en el sistema. Por lo tanto, se requiere implementar controles relacionados con la trazabilidad y auditoría de transacciones, conforme al componente actividades de control y al proceso DSS06, orientado a la gestión de controles de procesos de negocio.

Gestión de inventarios

Se identificó el riesgo de diferencias entre el inventario físico y el registrado en el sistema, originado por errores en el registro de las operaciones. Esta situación puede generar pérdidas económicas y afecta la confiabilidad de la información. El nivel de riesgo se considera alto, debido al impacto potencial en los resultados financieros. Este hallazgo evidencia la necesidad de aplicar conciliaciones periódicas y controles automatizados, en concordancia con el componente evaluación de riesgos y el proceso BAI03 relacionado con la gestión de soluciones tecnológicas.

Proceso de facturación

Se evidenció el riesgo de retrasos en la emisión de comprobantes, ocasionado por fallas en el sistema y la dependencia de validaciones manuales. Esta situación puede generar incumplimientos tributarios y afectar la eficiencia operativa. El nivel de riesgo es medio, debido a su menor probabilidad e impacto en comparación con otros procesos. Este hallazgo muestra la necesidad de fortalecer el componente información y comunicación mediante la automatización de procesos y la implementación de alertas, conforme al proceso DSS01.

Respaldos de información

Se identificó el riesgo de pérdida de información contable, debido a la ausencia de políticas formales de respaldo y recuperación de datos. Esta situación representa un nivel de riesgo alto, ya que puede afectar la continuidad operativa de la organización. Este resultado evidencia la necesidad de implementar políticas de respaldo y recuperación, en concordancia con el componente supervisión y el proceso DSS04 relacionado con la continuidad de los servicios.

Seguridad lógica

Se evidenció el riesgo asociado al uso compartido de credenciales, originado por la falta de políticas de seguridad informática. Esta situación dificulta la trazabilidad de las operaciones realizadas en el sistema y afecta la responsabilidad individual de los usuarios. El nivel de riesgo identificado es alto. Este hallazgo evidencia la necesidad de implementar políticas de control de acceso, autenticación y capacitación a los usuarios, conforme al componente ambiente de control y al proceso APO07.

Actualizaciones del sistema

Se identificó el riesgo de fallas operativas posteriores a las actualizaciones del sistema, debido a la inexistencia de pruebas previas. Esta situación puede generar interrupciones en el funcionamiento del sistema contable. El nivel de riesgo es medio. Este resultado muestra la necesidad de implementar procedimientos formales de gestión de cambios, conforme al componente actividades de control y al proceso BAI06.

Generación de reportes financieros

Se evidenció el riesgo de generación de reportes financieros incorrectos, originado por la configuración inadecuada de parámetros en el sistema. Esta situación puede afectar la toma de decisiones organizacionales. El nivel de riesgo identificado es alto. Este hallazgo evidencia la necesidad de establecer mecanismos de validación y control de la información generada, conforme al componente información y comunicación y al proceso MEA02.

4. Discusión

Los resultados evidencian que el sistema contable Odoo Community presenta un nivel favorable de control interno informático en relación con la definición de roles y permisos, debido a que la mayoría de los encuestados manifestó una percepción positiva sobre la existencia de controles de acceso. Este hallazgo coincide con lo señalado por Vincent Chang (2013), quien sostiene que los sistemas ERP contribuyen al fortalecimiento del control interno cuando disponen de perfiles de usuario claramente definidos y mecanismos de segregación de funciones. Sin embargo, la presencia de respuestas en niveles neutral y negativo indica que estos controles no se aplican de manera uniforme, lo que afecta la consistencia del ambiente de control, componente fundamental del modelo COSO (2017).

En relación con la identificación de riesgos informáticos, los resultados muestran que no todos los usuarios reconocen la existencia de procedimientos sistemáticos orientados a este propósito. Este resultado es consistente con lo planteado por Marco Vaca Benalcázar (2016), quien señala que la incorporación de tecnologías de información en los sistemas contables no siempre está acompañada de una adecuada gestión de riesgos. Esta situación representa una debilidad en el componente de evaluación de riesgos del control interno y se vincula con el proceso APO12 del marco ISACA (2019), el cual establece la necesidad de identificar, analizar y gestionar los riesgos asociados a las tecnologías de la información.

Los resultados relacionados con la detección de accesos no autorizados evidencian la existencia de percepciones diversas entre los encuestados, lo que refleja limitaciones en los mecanismos de monitoreo del sistema. Este hallazgo coincide con lo expuesto por Marshall Romney y Paul Steinbart (2021), quienes señalan que la protección de la información contable depende de la implementación de controles automatizados que permitan supervisar y registrar

las actividades realizadas en el sistema. La ausencia o debilidad de estos mecanismos afecta las actividades de control y limita la capacidad de prevenir o detectar oportunamente accesos no autorizados.

En cuanto a la confiabilidad de la información contable, los resultados reflejan una percepción mayoritariamente favorable, lo que indica que el sistema contribuye al procesamiento adecuado de los datos financieros. Este resultado coincide con lo señalado por Marco Govea Souza (2021), quien afirma que los sistemas ERP mejoran la calidad de la información financiera cuando se encuentran respaldados por controles internos adecuados. No obstante, la presencia de respuestas en niveles neutral y negativo sugiere que la confiabilidad de la información depende del nivel de implementación y supervisión de los controles informáticos.

Los resultados relacionados con las evaluaciones y revisiones periódicas evidencian debilidades en la supervisión del control interno informático. Este hallazgo es coherente con el modelo Committee of Sponsoring Organizations of the Treadway Commission (2017), el cual establece que la supervisión continua es un componente esencial para garantizar la efectividad del control interno. Asimismo, el marco COBIT 2019 señala, a través del dominio MEA01, la importancia del monitoreo permanente para asegurar el cumplimiento de los objetivos del sistema de información.

En conjunto, los resultados evidencian que el sistema contable Odoo Community dispone de funcionalidades que contribuyen al control interno informático, especialmente en aspectos relacionados con la gestión de accesos y la confiabilidad de la información. Sin embargo, se identifican debilidades en la gestión de riesgos y en la supervisión del sistema, lo que limita la efectividad del control interno. Estos hallazgos confirman la necesidad de fortalecer los mecanismos de evaluación de riesgos, monitoreo y supervisión, con el propósito de mejorar la seguridad del sistema y la confiabilidad de la información financiera.

5. Conclusiones

Los resultados de la encuesta evidencian que más del 60 % de los profesionales del área contable se ubican en los niveles de acuerdo y totalmente de acuerdo respecto a la adecuada definición de roles y permisos en el sistema ERP Odoo Community, lo que confirma la existencia de controles de acceso orientados a regular el uso del sistema. No obstante, la presencia de respuestas en niveles neutral y en desacuerdo, que representan entre el 20 % y el 30 % de los encuestados, demuestra que dichos controles no se aplican de manera uniforme en todos los procesos contables, lo que incrementa el riesgo asociado a una inadecuada segregación de funciones y a posibles afectaciones en la seguridad de la información.

En relación con la gestión de riesgos informáticos, se determinó que aproximadamente el 55 % de los encuestados reconoce la existencia de mecanismos de identificación de riesgos en el sistema contable, mientras que cerca del 45 % manifiesta percepciones neutrales o desfavorables. Este resultado evidencia una debilidad en el proceso de evaluación de riesgos del control interno informático, lo que incrementa la probabilidad de ocurrencia de eventos que pueden comprometer la integridad, confidencialidad y disponibilidad de la información contable, tales como accesos no autorizados, pérdida de datos o alteración de registros financieros.

Respecto a la supervisión y monitoreo del control interno informático, los resultados indican que menos del 50 % de los profesionales percibe la realización de evaluaciones y revisiones periódicas del sistema contable. Este hallazgo confirma la existencia de limitaciones en los procesos de supervisión, lo que reduce la capacidad de detectar oportunamente deficiencias en los controles implementados y afecta la efectividad del sistema para garantizar la confiabilidad de la información financiera generada por el ERP Odoo Community.

De manera general, se concluye que el sistema contable Odoo Community presenta un nivel moderado de control interno informático, debido a que cuenta con funcionalidades que contribuyen a la seguridad y confiabilidad de la información contable, pero presenta debilidades en la gestión de riesgos, la supervisión continua y la aplicación uniforme de los controles. Por lo tanto, es necesario fortalecer el control interno informático mediante la implementación de políticas, procedimientos y mecanismos de monitoreo alineados con estándares internacionales, con el fin de mejorar la protección de la información financiera y apoyar el proceso de auditoría contable.

Contribución de los autores: Conceptualización, PLA-M.; metodología SCM-M.; software, OCR-I.; validación, OCR-I.; redacción borrador original, y OMJ-X.; redacción, revisión y edición, OCR-I.; visualización, SCM-M.; supervisión PLA-M. Todos los autores han leído y aceptado la versión publicada todos del manuscrito.

Financiamiento: El proceso investigativo no ha recibido financiación externa.

Conflicto de intereses: Los autores declaran no tener ningún conflicto de intereses

Declaración de disponibilidad de los datos: Los datos están disponibles previa solicitud a los autores de correspondencia: rortega@uteq.edu.ec

Referencias Bibliográficas

Alcántara Hernández, L. J., Pérez López, J. A., y Morales Sánchez, M. E. (2023). The mediating effect of the internal control system on the relationship between the accounting information system and financial results. *UNAAA Ciencia, 2*(2), 45–60. https://doi.org/10.56926/unaaaciencia.v2i2.47

Arens, A. A., Elder, R. J., y Beasley, M. S. (2021). *Auditoría y aseguramiento* (16.ª ed.). Pearson.

Chang, S. I. (2013). Internal control framework for a compliant ERP system. *Information & Management, 50*(8), 532–543. https://doi.org/10.1016/j.im.2013.07.004

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO. https://www.coso.org

Deloitte. (2020). *Internal controls over financial reporting*. Deloitte Development LLC. https://www.deloitte.com

Gelinas, U. J., Dull, R. B., y Wheeler, P. R. (2018). *Accounting information systems* (11th ed.). Cengage Learning.

Govea Souza, J. A. (2021). Sistema de planificación de recursos empresariales (ERP) y su influencia en los procesos de negocio. *Producción y Gestión, 24*(1), 201–217. https://doi.org/10.15381/idata.v24i1.19831

Hall, J. A. (2022). *Accounting information systems* (11th ed.). Cengage Learning.

Huamán Heredia, A. D. (2022). Incidence of internal control in accounts receivable management. *Sapienza: International Journal of Interdisciplinary Studies, 3*(1), 818–829. https://doi.org/10.51798/sijis.v3i1.264

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security management systems*. https://www.iso.org/standard/27001

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA. https://www.isaca.org/resources/cobit

Laudon, K. C., y Laudon, J. P. (2022). *Management information systems: Managing the digital firm* (17th ed.). Pearson.

Mendoza, J. R., y Torres, L. M. (2020). Control interno y gestión de riesgos tecnológicos en sistemas contables. *Revista Científica FIPCAEC, 5*(18), 112–129. https://doi.org/10.23857/fipcaec.v5i18.204

Monk, E., y Wagner, B. (2013). *Concepts in enterprise resource planning* (4th ed.). Cengage Learning.

Odoo S.A. (2024). *Odoo documentation*. Odoo. https://www.odoo.com/documentation

Rojas Quispe, S. D., Castillo Vega, R. M., y Huamán López, P. A. (2026). El control interno y la facturación electrónica. *Ciencias Sociales y Económicas, 10*(1), 67–78. https://doi.org/10.18779/csye.v10i1.1135

Romney, M. B., y Steinbart, P. J. (2021). *Accounting information systems* (15th ed.). Pearson.

Sánchez Curiel, M. A., y Gómez Aguilar, N. (2019). Riesgos informáticos en los sistemas de información contable. *Contaduría y Administración, 64*(2), 1–21. https://doi.org/10.22201/fca.24488410e.2019.1817

Utami, M. P., y Kharisma, I. L. (2023). ERP implementation using Odoo software. *The Eastasouth Journal of Information System and Computer Science, 1*(2), 45–52. https://doi.org/10.58812/esiscs.v1i02.161

Vallejo Ballesteros, H. F., y Aguilar Wilca, L. S. (2024). Sistemas de información contable: Revisión sistemática. *RECIMUNDO,* *8*(3), 269–286. https://doi.org/10.26820/recimundo/8.(3).julio.2024.269-286

Weber, R. (2019). *Information systems control and audit*. Prentice Hall.

Wilkinson, J. W., Cerullo, M. J., Raval, V., y Wong-On-Wing, B. (2020). *Accounting information systems: Essential concepts and applications*. Wiley.