Maestría en Ciberseguridad y Seguridad de la Información

Propuesta de marco de gobernanza para el uso responsable de plataformas de inteligencia artificial en pymes de Costa Rica.

ESTUDIANTE:

Oscar Avila Madriz

PROFESORA:

Rebeca Esquivel

FECHA:

Abril, 2026

Declaración de derechos de Autor

Se declara que la presente investigación fue realizada íntegramente por su autor, Óscar Ávila, quien desarrolló el contenido de manera original y fundamentada, haciendo uso de diversas fuentes bibliográficas e institucionales debidamente citadas y referenciadas conforme a las normas APA. Durante el proceso se respetaron en todo momento los derechos de autor y propiedad intelectual de los documentos, marcos normativos y publicaciones analizadas.

El trabajo incorpora información proveniente de normas técnicas, marcos internacionales, artículos científicos y documentos oficiales, cuya integración se realizó con fines estrictamente académicos y siguiendo prácticas éticas de investigación.

Se autoriza el uso total o parcial de esta investigación como referencia para estudios académicos, científicos o profesionales futuros, siempre y cuando se cite adecuadamente la autoría correspondiente y se respeten los principios de integridad académica.

Dedicatoria y Agradecimientos

Agradezco profundamente a mi esposa, María Hernández Solís, por su apoyo constante, motivación y comprensión durante toda la maestría. A mi hija, Alice, cuyo amor ha sido el motor que me impulsó a iniciar y concluir esta maestría.

Extiendo mi agradecimiento a mis padres, Rosibel Madriz y Óscar Ávila, por inculcarme el valor del estudio, el esfuerzo y la disciplina; sin su acompañamiento, este logro no habría sido posible.

Agradezco también a mi patrono, Microsoft, por brindarme el apoyo financiero y la flexibilidad necesaria para continuar con mis estudios de posgrado. Agradezco especialmente a mi tutora, Rebeca Esquivel por su orientación académica, sus observaciones oportunas y el acompañamiento brindado durante el desarrollo de este trabajo.

Finalmente, expreso mi gratitud a los docentes y a la coordinación de la maestría por su guía académica y acompañamiento durante el programa.

Tabla de Contenido

Abstract

La adopción de inteligencia artificial (IA) en las pequeñas y medianas empresas (Pymes) costarricenses avanza con rapidez, pero sin lineamientos claros que orienten su uso responsable. Esta ausencia de gobernanza expone a las organizaciones a riesgos asociados con privacidad, sesgos algorítmicos, seguridad de la información y cumplimiento normativo. El objetivo de esta investigación es diseñar un marco de gobernanza para el uso responsable de plataformas de inteligencia artificial en las Pymes de Costa Rica, considerando sus limitaciones técnicas, organizativas y económicas.

Para ello, se desarrolló una revisión sistemática de literatura utilizando el proceso metodológico de Biolchini y consultas directas a fuentes institucionales oficiales. Se analizaron estándares internacionales como ISO/IEC 42001:2023, el NIST AI RMF (2023), el AI Act europeo, lineamientos éticos de la OCDE y la Estrategia Nacional de IA 2024–2027.

Los hallazgos evidencian la existencia de principios ampliamente aceptados como lo son la gestión del riesgo, transparencia, responsabilidad y ética, pero también una falta de guías prácticas adaptadas a las Pymes. A partir de estos hallazgos, se diseñó un marco de gobernanza estructurado en cinco componentes: gobernanza organizacional, gestión del riesgo de inteligencia artificial, ética y transparencia, protección de datos y seguridad de la información, y supervisión y mejora continua. La pertinencia y aplicabilidad del marco propuesto se validará mediante juicio de expertos con experiencia en ciberseguridad, gobernanza tecnológica e inteligencia artificial por eso se concluye que es necesario un modelo de gobernanza progresivo, accesible y contextualizado que permita a las Pymes implementar IA de manera segura, ética y alineada con estándares globales. Este trabajo establece las bases para su diseño, representando un aporte pertinente para el ecosistema empresarial costarricense.

Palabras clave: gobernanza de IA, Pymes, riesgo algorítmico, ética, marco de referencia, innovación, viabilidad, seguridad digital.

Capítulo 1. Introducción

1.1 Generalidades

La inteligencia artificial (IA) se ha consolidado como una tecnología transformadora en varios sectores como lo son los servicios financieros, los sectores de salud, el sector comercio y manufactura a nivel mundial, han generado grandes oportunidades en áreas como la automatización, el análisis de datos y la mejora de procesos de negocio.

En el caso de Costa Rica, esta transformación tecnológica comienza a evidenciarse también entre las pequeñas y medianas empresas (Pymes). Por ejemplo, según una encuesta promovida por Microsoft y realizada por Edelman DXL, cerca del 50 % de las Pymes costarricenses ya utilizan algún tipo de IA en sus operaciones cotidianas (Microsoft, 2024). De este porcentaje, un 48 % emplea el uso de la IA para mejorar el servicio al cliente y un 34 % para asegurar la continuidad del negocio.

Sin embargo, en Costa Rica, la adopción de IA en las pequeñas y medianas empresas (Pymes) aún enfrenta limitaciones asociadas a la falta de conocimiento especializado, la ausencia de marcos regulatorios específicos y la carencia de lineamientos de gobernanza que orienten su implementación segura y ética como lo demuestra un hallazgo donde se confirma que el 39 % de los empleados de Pymes utiliza herramientas de IA propias (no institucionales) ante la falta de políticas o recursos dentro de la organización (Microsoft, 2025). Esta práctica informal revela una carencia de gobernanza interna que puede exponer a las empresas a riesgos de seguridad y privacidad.

Las Pymes representan un sector clave para la economía costarricense, ya que constituyen la mayor fuerza del sector empresarial y son generadoras de empleo. Además, su papel es esencial para la competitividad nacional, ya que integran gran parte de las cadenas de suministro y participan activamente en sectores estratégicos de exportación. No obstante, su exposición a riesgos derivados del uso inadecuado de plataformas de IA como lo son las filtraciones de datos, sesgos en la toma de decisiones y vulnerabilidades de seguridad evidencia la necesidad de establecer un marco que promueva el uso responsable de estas tecnologías.

Por otro lado, es importante considerar que el ritmo acelerado de la transformación digital a nivel global puede aumentar la brecha tecnológica en Costa Rica si las Pymes no

cuentan con apoyo en términos de capacitación, inversión y lineamientos claros. En este contexto, la ausencia de un marco de gobernanza no solo afecta la seguridad, sino también la capacidad de las empresas para competir en igualdad de condiciones frente a organizaciones más grandes que ya cuentan con protocolos robustos.

La propuesta de investigación que se va a desarrollar se orienta hacia la propuesta de lineamientos estratégicos de gobernanza que fortalezcan la seguridad digital, al tiempo que favorezcan la innovación tecnológica en el sector de Pymes. De esta manera, se busca ofrecer una guía práctica que permita a las empresas adoptar la inteligencia artificial de forma ética, segura y sostenible, contribuyendo al fortalecimiento del ecosistema empresarial costarricense.

El presente anteproyecto se estructura de la siguiente manera: en primer lugar, se presentan los antecedentes, la definición del problema y la justificación que sustentan la investigación. Posteriormente, se establecen los objetivos, alcances y limitaciones del estudio, así como su viabilidad técnica, operativa y económica. El marco teórico fundamenta los conceptos de gobernanza de IA, gestión del riesgo algorítmico, ética y gobernanza tecnológica en Pymes. El marco metodológico describe el enfoque cualitativo y documental adoptado. Finalmente, se presenta la propuesta de marco de gobernanza de inteligencia artificial estructurada en cinco componentes, acompañada de herramientas prácticas de implementación, y se formulan las conclusiones y recomendaciones derivadas de la investigación.

1.2 Antecedentes del problema

El auge de la inteligencia artificial (IA) ha marcado un punto de inflexión en los procesos empresariales, permitiendo a las organizaciones optimizar tareas, mejorar la toma de decisiones y crear ventajas competitivas. Sin embargo, la implementación de estas tecnologías no está exenta de riesgos. En el caso de las Pymes, que representan más del 90% del sector productivo costarricense, la falta de marcos regulatorios claros y de estructuras internas de gobernanza expone a estas organizaciones a vulnerabilidades críticas, especialmente en el ámbito de la ciberseguridad.

A nivel internacional, se observa una tendencia creciente a establecer normativas y lineamientos éticos que regulen el uso de la IA. La Unión Europea, por ejemplo, ha trabajado en el AI Act, un marco normativo que busca garantizar la transparencia y la seguridad en el uso de estas tecnologías. Costa Rica, en contraste, carece de lineamientos específicos dirigidos a las Pymes, lo que genera un vacío en la gestión de riesgos asociados a la adopción de IA.

Un caso que ilustra los riesgos derivados de la ausencia de gobernanza interna sobre el uso de inteligencia artificial es el incidente reportado en Samsung Electronics en 2023, donde empleados ingresaron código fuente confidencial y notas de reuniones internas en ChatGPT, una de las inteligencias artificiales más utilizadas, lo que provocó la filtración involuntaria de información propietaria hacia servidores externos. Este evento, ampliamente documentado en medios especializados (Mashable, 2023), llevó a la empresa a prohibir temporalmente el uso de herramientas de IA generativa entre su personal. Aunque se trata de una corporación de gran escala, el incidente resulta especialmente relevante para las Pymes, ya que estas organizaciones suelen carecer de los controles, políticas y mecanismos de detección necesarios para prevenir situaciones similares, lo que las expone a un nivel de riesgo proporcionalmente mayor.

Los antecedentes muestran también que, en la región latinoamericana, las brechas en infraestructura tecnológica, capacitación en ciberseguridad y acceso a herramientas de cumplimiento normativo representan barreras adicionales. Esto provoca que, aunque las Pymes reconozcan el valor estratégico de la IA, muchas veces la implementen sin procesos de gobernanza adecuados, aumentando el riesgo de incidentes como filtraciones de datos, sesgos en la toma de decisiones automatizadas y dependencia excesiva de proveedores externos.

En el ámbito legal costarricense, el marco normativo aplicable al uso de datos e inteligencia artificial se sustenta principalmente en la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales y su reglamento, así como en la Estrategia Nacional de Inteligencia Artificial 2024–2027 (ENIA-CR). No obstante, ninguno de estos instrumentos establece lineamientos operativos específicos para la gobernanza de IA en el sector empresarial privado, particularmente en las Pymes. Esta brecha normativa constituye uno de los vacíos que la presente investigación busca abordar mediante la propuesta de un marco de gobernanza adaptado.

1.3 Definición y descripción del problema

Actualmente en Costa Rica las Pymes que incursionan en el uso de plataformas de inteligencia artificial carecen de guías o modelos de referencia que orienten su implementación de forma segura y ética. De hecho, según la Estrategia Nacional de Inteligencia Artificial de Costa Rica (ENIA-CR), uno de sus retos principales es la carencia de marcos normativos específicos que regulen el uso, adopción y desarrollo responsable de la IA en los distintos sectores del país (MICITT, 2024).

Dado el carácter emergente de esta tecnología esta situación genera múltiples problemáticas como lo son:

- La ausencia de regulación específica, ya que no existen políticas ni marcos nacionales que regulen el uso de IA en el ámbito empresarial privado. La ENIA-CR plantea explícitamente la necesidad de elaborar un marco normativo que incluya pautas técnicas y éticas para la IA en Costa Rica (MICITT, 2024).
- Riesgo de filtración de datos sensibles, ya que el uso de plataformas de IA sin un marco de control adecuado aumenta la exposición a incidentes de ciberseguridad.
- Falta de lineamientos de gobernanza, debido a que actualmente las Pymes no cuentan con protocolos para establecer roles, responsabilidades y buenas prácticas en torno a la implementación de IA.
- Desconocimiento técnico y ético ya que muchas empresas adoptan herramientas de IA sin valorar los riesgos relacionados con privacidad y el uso indebido de información.

Estos factores reducen la confianza de los distintos actores (clientes, empleados, reguladores) en la adopción de IA y pueden generar impactos negativos tanto económicos como reputacionales. Por ejemplo, modelos de IA sin supervisión adecuada pueden producir decisiones sesgadas o discriminatorias, lo que puede derivar en litigios, sanciones o pérdida de reputación.

Como consecuencia de estas deficiencias estructurales, surge la necesidad de desarrollar un marco de gobernanza que establezca principios y directrices claras para el uso responsable de IA en este sector. Este vacío regulatorio y de gobernanza resulta aún más grave en un entorno global donde los estándares y políticas de IA están emergiendo rápidamente y donde se advierte que la falta de normativa puede obstaculizar la adopción segura en empresas de menor escala.

1.4 Justificación

La pertinencia del proyecto radica en que la IA es una de las tecnologías con mayor impacto en la transformación digital, pero su implementación sin un marco de gobernanza conlleva riesgos significativos. En el caso de las Pymes costarricenses, la ausencia de lineamientos concretos limita su capacidad de garantizar el uso responsable y seguro de la IA.

Este trabajo se justifica porque:

1. **Fortalece la ciberseguridad organizacional.** Un marco de gobernanza permitirá reducir riesgos de ataques dirigidos a sistemas basados en IA, como manipulación de algoritmos o explotación de vulnerabilidades en modelos de aprendizaje automático.

2. **Contribuye a la ética empresarial.** La gobernanza asegura que las decisiones automatizadas respeten los principios de equidad, transparencia y privacidad.

3. **Apoya la competitividad de las Pymes.** Al adoptar prácticas de gobernanza alineadas con estándares internacionales, las empresas estarán en mejores condiciones de competir en mercados donde clientes y aliados valoran la seguridad y la confianza digital.

4. **Genera impacto académico y práctico.** El proyecto combina marcos teóricos internacionales con un análisis del contexto nacional, aportando tanto al conocimiento académico como a la formulación de lineamientos aplicables.

En resumen, se trata de una propuesta con un alto valor estratégico que vincula la ciberseguridad con la transformación digital de las Pymes.

1.5 Viabilidad

A continuación, se define la viabilidad de esta propuesta.

1.5.1 Punto de vista técnico. El desarrollo del proyecto es factible dado que la investigación se fundamenta en fuentes confiables de literatura académica y estándares reconocidos como la ISO/IEC 27001 o el marco NIST AI RMF. Además, en esta investigación no se realiza una implementación, ya que solamente es una propuesta basada en analizar y adaptar lineamientos ya existentes a la realidad de las Pymes costarricenses.

1.5.2. Punto de vista operativo. La investigación se desarrollará bajo un enfoque documental y estratégico, sustentado en la revisión y análisis de marcos internacionales de gobernanza de inteligencia artificial. La validación del marco propuesto se realizará mediante juicio de expertos, con el fin de evaluar su pertinencia, coherencia y aplicabilidad en el contexto de las Pymes costarricenses. Este enfoque no requiere acceso directo a empresas ni intervención en procesos operativos reales, lo que garantiza su viabilidad operativa dentro del alcance académico del proyecto.

1.5.3. Punto de vista económico. Los costos asociados se limitan a herramientas de análisis, material didáctico y al tiempo del investigador. El desarrollo de esta propuesta no requiere de la compra o alquiler de ningún equipo. No implica inversiones de capital

significativas ni pruebas piloto en empresas reales. Por tanto, este proyecto es sostenible económicamente.

1.6 Objetivos

Para la formulación de los objetivos de este proyecto se eligió la Taxonomía de Bloom, ya que es reconocida internacionalmente como una de las metodologías más utilizadas para la definición de objetivos de investigación. Esta taxonomía permite estructurar los objetivos en niveles de complejidad cognitiva que van desde recordar y comprender hasta analizar, evaluar y crear.

Debido a los puntos mencionados anteriormente, los objetivos de la investigación se formularon de acuerdo con los niveles superiores de la taxonomía, de modo que se alcance progresivamente el objetivo general a través de la aplicación, el análisis, la evaluación y la creación.

1.6.1 Objetivo general

Diseñar un marco de gobernanza para el uso responsable de plataformas de inteligencia artificial en las pequeñas y medianas empresas costarricenses, alineado con estándares internacionales y adaptado a sus capacidades técnicas, organizacionales y financieras.

1.6.2 Objetivos específicos

1. Identificar y analizar los principales marcos y modelos internacionales de gobernanza de inteligencia artificial, tales como el NIST Artificial Intelligence Risk Management Framework, la norma ISO/IEC 42001:2023, el Artificial Intelligence Act de la Unión Europea, con el fin de determinar su aplicabilidad al contexto de las pequeñas y medianas empresas costarricenses.
2. Analizar los riesgos éticos, legales, técnicos y de seguridad de la información asociados a la adopción de inteligencia artificial en las Pymes de Costa Rica, considerando sus limitaciones operativas, organizacionales y de madurez digital.
3. Desarrollar el marco de gobernanza institucional que incluya políticas, lineamientos éticos y controles de seguridad específicos para la realidad operativa de las Pymes.
4. Validar la pertinencia, viabilidad y aplicabilidad del marco de gobernanza propuesto, mediante el juicio de expertos, quienes evaluarán la claridad, viabilidad y coherencia del marco diseñado, considerando su aplicabilidad en el sector Pyme costarricense.

1.7 Alcances y limitaciones

Alcances

La investigación aborda la gobernanza de inteligencia artificial desde tres dimensiones principales:

1. Ética, enfocada en sesgos algorítmicos, transparencia y responsabilidad.
2. Legal, considerando el cumplimiento de la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales y lineamientos internacionales relevantes.
3. Técnica, centrada en la gestión del riesgo, protección de datos y controles de seguridad asociados al uso de plataformas de IA.

Alcance poblacional:

El estudio se enfoca en pequeñas y medianas empresas (Pymes) costarricenses, particularmente en los sectores de servicios y comercio, por ser los principales adoptantes de herramientas de inteligencia artificial en el país.

Alcance tecnológico:

La investigación prioriza el análisis de plataformas de inteligencia artificial de terceros, incluyendo herramientas de IA generativa y sistemas automatizados de apoyo a la toma de decisiones, que representan las soluciones de mayor accesibilidad para las Pymes.

Alcance del entregable:

El producto final consistirá en una propuesta estructurada de marco de gobernanza de IA, acompañada de lineamientos estratégicos y una matriz preliminar de riesgos, diseñada para ser adaptable a la realidad operativa de las Pymes costarricenses.

Limitaciones

La investigación presenta las siguientes limitaciones:

Limitación técnica:
El trabajo se desarrolla a nivel estratégico y normativo. No incluye el desarrollo de software, programación de algoritmos, configuración de infraestructura tecnológica ni implementación técnica de controles de seguridad específicos.

Limitación metodológica:
Debido a restricciones de tiempo y alcance académico, la validación del marco se realizará

mediante juicio de expertos y no a través de una implementación prolongada en empresas piloto.

Limitación geográfica:
El estudio se centra exclusivamente en el contexto normativo y socioeconómico de Costa Rica. Su aplicación en otros países requeriría ajustes legales y regulatorios.

Limitación normativa y temporal:
El análisis se fundamenta en la legislación y estándares vigentes al momento de la investigación. Dado el carácter dinámico de la inteligencia artificial y su regulación, futuros cambios legislativos o tecnológicos podrían requerir actualizaciones del marco propuesto.

1.8 Marco de referencia organizacional y socioeconómico

Como se detalló en los alcances de la investigación, el trabajo se enfoca en el diseño de un marco de gobernanza de inteligencia artificial dirigido específicamente a pequeñas y medianas empresas (Pymes) costarricenses, particularmente en los sectores de servicios y comercio. Por esta razón, no se desarrolla el estudio en una organización específica, sino que se construye una propuesta adaptable a este segmento empresarial, considerando sus características operativas, limitaciones técnicas y contexto socioeconómico.

En consecuencia, el marco de referencia organizacional no describe una empresa en particular, sino el entorno general en el que operan las Pymes costarricenses y las condiciones que influyen en la adopción de tecnologías de inteligencia artificial dentro de este sector.

1.8.1 Historia

En las últimas dos décadas, las Pymes han consolidado su papel como el principal motor económico de Costa Rica. Según datos del Ministerio de Economía, Industria y Comercio (MEIC), representan más del 95% de las empresas registradas y generan una parte significativa del empleo formal. Tradicionalmente, estas organizaciones han operado en sectores como comercio, servicios y manufactura ligera, aunque en los últimos años ha crecido la presencia de Pymes vinculadas a la tecnología y la transformación digital.

Durante este proceso de modernización, muchas Pymes han comenzado a incorporar herramientas de inteligencia artificial para tareas como lo son la atención automatizada, el análisis de datos y la optimización de procesos operativos. No obstante, este avance no siempre ha estado acompañado por una adecuada estructura de gobernanza o políticas de control ético y de seguridad de la información. Esta situación ha generado un vacío que motiva el presente trabajo dado a la necesidad de establecer un marco de gobernanza flexible, práctico y adaptado a la realidad de las Pymes costarricenses.

1.8.2 Tipo de negocio y mercado meta

Las Pymes costarricenses se caracterizan por su diversidad en tamaño, sector y grado de digitalización. Su mercado meta suele centrarse en consumidores nacionales o regionales, con una fuerte orientación hacia la prestación de servicios personalizados. Sin embargo, la competitividad global y el acceso creciente a soluciones tecnológicas impulsan a muchas Pymes a adoptar herramientas digitales avanzadas, incluyendo sistemas de IA en áreas como mercadeo, análisis de datos, atención al cliente y automatización de tareas.

Pese a ello, la mayoría carece de departamentos especializados en tecnologías de información o ciberseguridad, lo que conlleva riesgos en la protección de datos. Esta realidad confirma la necesidad de un modelo de gobernanza que oriente y estandarice las buenas prácticas, sin importar el tipo o tamaño de la empresa.

1.8.3 Misión, visión y valores

Dado que el marco propuesto no se dirige a una empresa particular, sino a las Pymes en general, se presenta a continuación una guía orientativa.

Misión: Promover el uso responsable, ético y seguro de la inteligencia artificial en las Pymes costarricenses, impulsando su transformación digital con base en principios de transparencia, equidad y confianza.

Visión: Lograr que las Pymes de Costa Rica adopten tecnologías de inteligencia artificial de forma sostenible y conforme a estándares internacionales de gobernanza y ciberseguridad, fortaleciendo su competitividad e innovación.

Valores: Responsabilidad, integridad, ética tecnológica, seguridad, respeto por la privacidad y compromiso con la mejora continua.

Estos principios orientan tanto la formulación del marco de gobernanza como su posible adopción por cualquier organización interesada en incorporar la inteligencia artificial de forma consciente y regulada.

1.8.4 Políticas institucionales

En Costa Rica las políticas institucionales relacionadas con inteligencia artificial se encuentran en desarrollo. La Estrategia Nacional de Inteligencia Artificial 2024–2027 (ENIA-CR) establece los primeros lineamientos generales para impulsar el uso responsable de la IA en el país, priorizando la innovación, la capacitación del talento humano y la protección de los derechos digitales. Sin embargo, aún no existen guías específicas para las Pymes en materia de gobernanza, evaluación de riesgos o cumplimiento ético.

La ausencia de políticas formales dentro del sector privado, especialmente en pequeñas y medianas empresas, representa un desafío y una oportunidad. La presente investigación busca contribuir a cerrar esa brecha mediante una propuesta adaptable que sirva como referencia para la formulación de políticas internas de gobernanza en IA, con un enfoque progresivo y económicamente accesible para las Pymes, alineado a estándares internacionales como el NIST AI Risk Management Framework y la ISO/IEC 42001.

En conclusión, este marco de referencia no se limita a una organización particular, sino que pretende reflejar la realidad de las Pymes costarricenses, sus limitaciones estructurales y su potencial de innovación.

1.9 Revisión sistemática de la literatura y estado de la Cuestión

El propósito de esta revisión es identificar modelos, marcos y buenas prácticas de gobernanza de inteligencia artificial aplicables al contexto de las pequeñas y medianas empresas (Pymes) costarricenses.

La revisión se desarrolló conforme al proceso metodológico propuesto por Biolchini, Gomes, Cruz y Horta (2005) para la elaboración de revisiones sistemáticas en ingeniería. Este proceso incluye las etapas de definición del problema, establecimiento de preguntas de investigación, planificación de la estrategia de búsqueda, aplicación de criterios de inclusión y exclusión, extracción de información relevante y síntesis de los resultados.

El uso de esta metodología garantiza un procedimiento estructurado, reproducible y orientado a la trazabilidad, lo cual fortalece la validez académica del estado de la cuestión

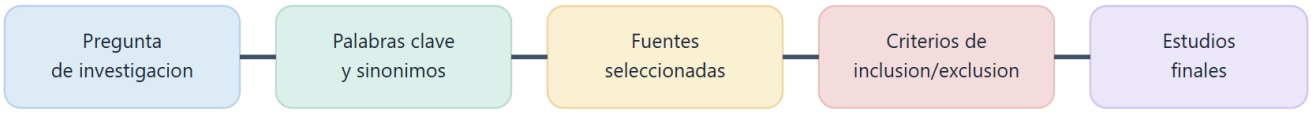
presentado en este capítulo.
A continuación, se detallan las etapas seguidas en el proceso.

1.9.1 Planificación de la revisión

La etapa de planificación consistió en definir la estrategia general de búsqueda, los motores de búsqueda a utilizar, el alcance temporal, los criterios de selección y las palabras clave relevantes para la temática de la gobernanza de IA en Pymes.

Para la búsqueda documental se utilizó Google Scholar por su cobertura amplia, acceso libre y pertinencia para investigaciones académicas en ciencias computacionales, ciberseguridad e inteligencia artificial. Su uso garantiza que las fuentes recolectadas sean verificables, indexadas y adecuadas para estudios de posgrado. Adicionalmente, se incluyeron fuentes institucionales oficiales que, por su naturaleza normativa, no se encuentran indexadas en Google Scholar, pero que son indispensables para el análisis del contexto costarricense. Estas fuentes se consultaron directamente desde los portales oficiales de las instituciones correspondientes, como el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) para la *Estrategia Nacional de Inteligencia Artificial 2024–2027 (ENIA-CR)*. Su incorporación responde a su relevancia como documento rector para el desarrollo de la inteligencia artificial en Costa Rica, aunque no forman parte del conjunto de resultados arrojado por el motor académico de búsqueda.

Durante esta fase también se determinó que la revisión se enfocaría en literatura publicada entre 2018 y 2025, debido al rápido avance de los marcos de gobernanza y ética en IA, y la relevancia de incluir estándares recientes como ISO/IEC 42001:2023 y el NIST AI RMF 1.0.



Proceso metodológico de la revisión sistemática de literatura. Fuente: Elaboración propia a partir de Biolchini et al. (2005).

1.9.1.1 Formulación de la pregunta de investigación

La pregunta formulada para esta revisión sistemática es la siguiente:

¿Qué marcos, lineamientos o buenas prácticas de gobernanza de inteligencia artificial pueden adaptarse al contexto de las pequeñas y medianas empresas en Costa Rica, considerando sus capacidades técnicas, organizacionales y financieras?

1.9.1.2 Palabras clave y sinónimos

Durante la búsqueda se utilizaron palabras clave y términos relacionados con el Proyecto que permitieran abarcar estudios tanto en español como en inglés:

- AI governance
- Artificial intelligence governance
- AI risk management framework
- Responsible AI
- Governance framework SMEs
- Gobernanza de inteligencia artificial
- Inteligencia artificial en Pymes
- ISO 42001 governance
- NIST AI RMF
- Ethical AI principles

Estas palabras clave se combinaron utilizando operadores booleanos (AND, OR) para mejorar la precisión de los resultados.

1.9.1.3 Selección de fuentes

La identificación de fuentes se realizó mediante búsquedas sucesivas en Google Scholar utilizando las palabras clave definidas. Posteriormente, se analizaron los títulos, resúmenes y descriptores de cada resultado para determinar su pertinencia con la pregunta de investigación.

Se integraron fuentes pertenecientes a cuatro categorías principales:

1. **Marcos técnicos y normativos internacionales:**
    - *NIST Artificial Intelligence Risk Management Framework (2023)*

- *ISO/IEC 42001:2023 – Artificial Intelligence Management System*

2. **Regulación internacional:**
    - *Artificial Intelligence Act (Unión Europea)*
3. **Lineamientos éticos y clasificación de IA:**
    - *OECD Framework for the Classification of AI Systems*
    - *The Global Landscape of AI Ethics Guidelines* (Jobin, Ienca & Vayena, 2019)
4. **Política pública nacional:**
    - *Estrategia Nacional de Inteligencia Artificial 2024–2027 (ENIA-CR)*

Estas fuentes constituyen la base documental necesaria para analizar el estado actual de la gobernanza de IA a nivel internacional y su aplicabilidad al contexto costarricense.

1.9.1.4 Definición del problema de investigación

La gobernanza de la inteligencia artificial (IA) se ha convertido en un componente crítico para las organizaciones que buscan adoptar esta tecnología de manera ética, segura y conforme a las normativas internacionales. En el caso de las Pymes costarricenses, la ausencia de políticas claras y de marcos de control adaptados limita la adopción responsable de soluciones basadas en IA.

El problema que guía esta investigación consiste en la falta de un marco de gobernanza de inteligencia artificial ajustado a la realidad operativa y socioeconómica de las Pymes costarricenses.

1.9.1.5 Criterios de inclusión y exclusión

Para garantizar la calidad y pertinencia de la información recopilada, establecí los siguientes criterios:

Inclusión:

- Documentos académicos o técnicos con revisión por pares.
- Guías, normas o marcos de referencia sobre gobernanza o gestión del riesgo en IA.

- Estudios aplicables a pequeñas o medianas empresas, o a entornos con recursos limitados.
- Publicaciones entre 2018 y 2025, en inglés o español.

Exclusión:

- Documentos de opinión sin respaldo metodológico.
- Publicaciones sin acceso al texto completo.
- Trabajos centrados exclusivamente en corporaciones de gran escala.

1.9.1.6 Estudios seleccionados

Luego de aplicar los criterios anteriores, seleccioné seis fuentes que representan los marcos más relevantes para construir un modelo de gobernanza de IA:

Titulo	Estrategia Nacional de Inteligencia Artificial 2024–2027 (ENIA-CR)
Autor(es)	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)
Año	2024
Tipo de documento	Estrategia nacional
URL oficial	https://micitt.go.cr
Temas revisados	Ejes estratégicos relacionados con ética, uso responsable y desarrollo de talento.
Relevancia para la investigación	Proporciona el marco nacional de referencia para el uso de IA en Costa Rica; sustenta la importancia de adaptar modelos para Pymes.

Titulo	Artificial Intelligence Risk Management Framework (AI RMF 1.0)
Autor(es)	Instituto Nacional de Estándares y Tecnología (NIST)
Año	2023
Tipo de documento	Marco técnico / gestión del riesgo
URL oficial	https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
Temas revisados	Funciones de gobernar, mapear, medir y gestionar; lineamientos de riesgo algorítmico.
Relevancia para la investigación	Base estructural para definir el ciclo de gobernanza de IA adaptado a Pymes.

Titulo	Artificial Intelligence Act (AI Act)
Autor(es)	Unión Europea
Año	2024
Tipo de documento	Regulación legal / marco normativo
URL oficial	https://artificialintelligenceact.eu/
Temas revisados	Artículos 5–12: clasificación por niveles de riesgo, obligaciones de transparencia, gobernanza.
Relevancia para la investigación	Permite adaptar principios regulatorios europeos al contexto costarricense de manera proporcional.

Titulo	ISO/IEC 42001:2023 – Artificial Intelligence Management System
Autor(es)	ISO/IEC
Año	2023
Tipo de documento	Norma internacional
URL oficial	https://www.iso.org/standard/42001

Temas revisados	Requisitos del sistema de gestión de IA: liderazgo, planificación, soporte, operación y mejora.
Relevancia para la investigación	Modelo formal de gestión que inspira la propuesta, aunque requiere simplificación para Pymes.

Titulo	OECD Framework for the Classification of AI Systems
Autor(es)	Organización para la Cooperación y el Desarrollo Económico (OCDE)
Año	2022
Tipo de documento	Informe técnico
URL oficial	https://oecd.ai/en/classification
Temas revisados	Clasificación de IA según autonomía, propósito, impacto y riesgo.
Relevancia para la investigación	Ayuda a comprender los tipos de IA que pueden requerir diferentes niveles de gobernanza.

Titulo	The Global Landscape of AI Ethics Guidelines
Autor(es)	Jobin, A.; Ienca, M.; & Vayena, E.
Año	2019
Tipo de documento	Artículo académico
URL oficial	https://www.nature.com/articles/s42256-019-0088-2
Temas revisados	Análisis comparativo de 80 guías éticas de IA; principios de transparencia, equidad, responsabilidad.
Relevancia para la investigación	Aporta la base ética universal que complementa el componente técnico del marco.

1.9.1.7 Documentación de los resultados

El proceso de búsqueda en Google Scholar arrojó inicialmente más de 150 resultados, entre artículos académicos, informes y documentos institucionales. Tras aplicar los criterios de inclusión y exclusión, se eliminaron duplicados, fuentes sin relevancia para Pymes y documentos sin enfoque en gobernanza de IA.

Finalmente, se seleccionaron seis documentos clave, debido a: su reconocimiento internacional, su aplicabilidad práctica, su relevancia conceptual para gobernanza, riesgo y ética, su potencial de adaptación al contexto costarricense.

Capítulo 2. Marco Teórico o Conceptual

El presente capítulo tiene como propósito fundamentar teóricamente la propuesta de investigación, estableciendo los conceptos, enfoques y marcos de referencia que sustentan el desarrollo de un modelo de gobernanza de inteligencia artificial (IA) aplicable a las pequeñas y medianas empresas (Pymes) costarricenses.

A partir de la revisión sistemática de la literatura, se identificaron cuatro ejes conceptuales principales: gobernanza de la IA, gestión del riesgo algorítmico, ética y responsabilidad en IA, y gobernanza tecnológica en Pymes. Adicionalmente, se presenta un análisis comparativo de los marcos internacionales de referencia que sustenta el diseño del marco propuesto.

2.1 Gobernanza de la inteligencia artificial

La gobernanza de la inteligencia artificial se refiere al conjunto de principios, estructuras, procesos y mecanismos que aseguran que los sistemas de IA sean desarrollados, implementados y utilizados de manera responsable, ética, segura y conforme a las regulaciones vigentes. Según el NIST (2023), la gobernanza implica la capacidad de una organización para gestionar los riesgos de los sistemas de IA durante todo su ciclo de vida, desde el diseño hasta la operación.

La gobernanza no debe entenderse únicamente como un requisito técnico o normativo, sino como una práctica estratégica que permite alinear la innovación tecnológica con los valores institucionales y los derechos de las personas. En el caso de las Pymes, la gobernanza de IA debe adoptar un enfoque proporcional, es decir, ajustado a sus capacidades y recursos,

pero que garantice la transparencia y la rendición de cuentas. En la literatura que utilizamos para la investigación se identifican dos enfoques predominantes de gobernanza de IA:

1. **Enfoque descendente (top-down):** Promovido por marcos regulatorios como el AI Act de la Unión Europea, este enfoque establece obligaciones desde la autoridad reguladora hacia las organizaciones, incluyendo clasificación de riesgo, requisitos de transparencia y mecanismos de supervisión. Su principal ventaja es la consistencia normativa, pero puede resultar complejo y costoso para organizaciones pequeñas (Unión Europea, 2024).

2. **Enfoque ascendente (bottom-up):** Presente en marcos como el NIST AI RMF, este enfoque promueve la adopción voluntaria de buenas prácticas a partir de la cultura organizacional, la evaluación interna de riesgos y la mejora continua. Es más flexible y adaptable, lo que lo hace particularmente relevante para Pymes que no están sujetas a regulaciones formales de IA (NIST, 2023).

Para el contexto de las Pymes costarricenses, se considera pertinente un enfoque híbrido que combine elementos de ambas perspectivas: la estructura y los principios del enfoque regulatorio con la flexibilidad y proporcionalidad del enfoque voluntario.

2.2 Gestión del riesgo en sistemas de inteligencia artificial

La gestión del riesgo constituye un componente esencial de la gobernanza de la inteligencia artificial. El Instituto Nacional de Estándares y Tecnología (NIST, 2023), a través del Artificial Intelligence Risk Management Framework (AI RMF 1.0), establece cuatro funciones fundamentales para la gestión del riesgo en sistemas de IA:

1. **Gobernar (Govern):** Establece la cultura organizacional, los roles, las responsabilidades y las políticas necesarias para gestionar los riesgos de IA. Esta función es transversal y sustenta a las demás.

2. **Mapear (Map):** Identifica y contextualiza los riesgos asociados a los sistemas de IA dentro de la organización, considerando el entorno operativo, los datos utilizados, las partes interesadas y los posibles impactos.

3. **Medir (Measure):** Evalúa y cuantifica los riesgos identificados mediante métricas, pruebas y análisis que permitan determinar su probabilidad e impacto.

4. **Gestionar (Manage):** Implementa acciones de mitigación, monitoreo y respuesta para los riesgos evaluados, incluyendo controles técnicos, operativos y de supervisión.

Por otra parte, la norma ISO/IEC 42001:2023 aborda la gestión del riesgo desde la perspectiva de un sistema de gestión formal, estableciendo requisitos en sus cláusulas 6.1 (acciones para abordar riesgos y oportunidades) y en el Anexo A (controles de referencia). Este enfoque, si bien es más estructurado, está diseñado para organizaciones con mayor madurez en sus procesos de gestión.

El AI Act de la Unión Europea (2024) introduce un enfoque basado en niveles de riesgo, clasificando los sistemas de IA en cuatro categorías: riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo. Esta clasificación determina las obligaciones de cumplimiento aplicables a cada tipo de sistema.

La siguiente tabla presenta una comparación de cómo cada marco internacional aborda la gestión del riesgo:

Dimensión	NIST AI RMF	ISO/IEC 42001	AI Act (UE)	OCDE
Enfoque del riesgo	Funcional (4 funciones)	Basado en sistema de gestión	Por niveles de riesgo	Por clasificación de sistemas
Obligatoriedad	Voluntario	Certificable	Regulatorio obligatorio (UE)	Recomendaciones
Nivel de detalle operativo	Alto	Alto	Medio-Alto	Medio
Adaptabilidad a Pymes	Alta (flexible)	Baja (requiere simplificación)	Baja (diseñado para proveedores)	Media
Ciclo de vida cubierto	Completo	Completo	Focalizado en alto riesgo	General

Fuente: Elaboración propia a partir de NIST (2023), ISO/IEC (2023), Unión Europea (2024) y OCDE (2022).

Para las Pymes costarricenses, se considera esencial implementar mecanismos básicos de evaluación de riesgo que no requieran una infraestructura compleja. Esto puede lograrse mediante cuestionarios de madurez, listas de verificación y la documentación mínima del ciclo de vida de los sistemas de IA. La integración de esta práctica no solo mitiga riesgos operativos y legales, sino que también fortalece la confianza de los clientes y socios comerciales.

2.3 Ética y principios de IA responsable

La ética en la inteligencia artificial constituye uno de los pilares más relevantes del marco conceptual. Diversos organismos internacionales, como la Comisión Europea, la OCDE y múltiples instituciones académicas, establecen principios fundamentales que deben guiar el desarrollo y uso de sistemas inteligentes.

En un estudio de referencia para este campo, Jobin, Ienca y Vayena (2019) realizaron un análisis comparativo de 84 guías éticas de IA publicadas a nivel mundial, identificando once principios recurrentes:

1. Transparencia
2. Justicia y equidad
3. No maleficencia
4. Responsabilidad
5. Privacidad
6. Beneficencia
7. Libertad y autonomía
8. Confianza
9. Sostenibilidad
10. Dignidad
11. Solidaridad

De estos principios, los más relevantes para el contexto de las Pymes costarricenses son la transparencia, la responsabilidad, la equidad, la privacidad y la no maleficencia, ya que se vinculan directamente con los riesgos identificados en el uso de plataformas de IA por parte de organizaciones con recursos limitados.

En el entorno Pyme costarricense, es fundamental que las políticas internas incluyan lineamientos de ética digital, uso responsable de datos y evaluación de impacto algorítmico. Estos elementos aseguran que la IA se implemente con justicia, respeto y responsabilidad social, independientemente del tamaño de la organización.

2.4 Gobernanza tecnológica en Pymes costarricenses

Las pequeñas y medianas empresas costarricenses enfrentan desafíos particulares en materia de gobernanza tecnológica. Según el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (2024), las Pymes representan más del 95% del tejido empresarial nacional, pero presentan limitaciones significativas en diversas dimensiones:

Infraestructura digital: La mayoría opera con recursos tecnológicos básicos y no cuenta con servidores dedicados, plataformas de gestión empresarial integradas ni herramientas especializadas de ciberseguridad.

Talento humano: Pocas Pymes disponen de personal especializado en tecnologías de información, ciberseguridad o ciencia de datos. Las funciones tecnológicas suelen recaer en personal con formación en otras áreas.

Presupuesto para tecnología: La inversión en infraestructura y herramientas tecnológicas compite con otras prioridades operativas, lo que limita la capacidad de adoptar soluciones de gobernanza complejas.

Cultura organizacional: En muchas Pymes, las decisiones sobre tecnología se toman de forma reactiva y no estratégica, sin procesos formales de evaluación, documentación o supervisión.

Los datos de Microsoft (2025) confirman esta tendencia en el contexto costarricense, al reportar que el 39% de los empleados de Pymes utiliza herramientas de IA propias ante la falta de políticas o recursos dentro de la organización.

En este contexto, se propone concebir la gobernanza tecnológica como un proceso gradual que permita a las Pymes avanzar desde la informalidad hacia prácticas más estructuradas de control y transparencia. La implementación de un marco de gobernanza de IA adaptado a este entorno permitirá fortalecer la protección de datos, el cumplimiento regulatorio y la competitividad, alineándose con los objetivos de la Estrategia Nacional de Inteligencia Artificial 2024–2027 (MICITT, 2024).

2.5 Análisis comparativo de marcos internacionales de gobernanza de IA

Con el fin de sustentar la propuesta de marco de gobernanza y evidenciar las brechas que justifican su diseño, se presenta un análisis comparativo de los principales marcos

internacionales revisados. Esta comparación permite identificar los elementos comunes, las diferencias en sus enfoques y su nivel de aplicabilidad al contexto de las Pymes costarricenses.

Criterio	NIST AI RMF 1.0	ISO/IEC 42001:2023	AI Act (UE)	OCDE	ENIA-CR
Tipo de instrumento	Marco voluntario	Norma certificable	Regulación obligatoria	Recomendaciones	Estrategia nacional
Alcance geográfico	Estados Unidos	Internacional	Unión Europea	Internacional	Costa Rica
Enfoque principal	Gestión del riesgo	Sistema de gestión	Regulación por riesgo	Clasificación y principios	Política pública
Componentes éticos	Integrados en GOVERN	Política de IA (5.2)	Arts. 13-14 transparencia	5 principios éticos	Eje de ética
Gestión del riesgo	4 funciones detalladas	Cláusula 6.1 + Anexo A	Clasificación 4 niveles	Clasificación por impacto	General/estratégico
Gobernanza organizacional	Roles y cultura	Liderazgo y planificación	Obligaciones por actor	Rendición de cuentas	Talento humano
Aplicabilidad a Pymes	**Alta** (flexible, escalable)	**Baja** (requiere adaptación significativa)	**Baja** (enfocado en proveedores/alto riesgo)	**Media** (principios generales)	**Baja** (sin guías operativas para Pymes)
Costo de implementación	Bajo	Alto (certificación)	Alto (cumplimiento legal)	Bajo	N/A

Fuente: Elaboración propia a partir de NIST (2023), ISO/IEC (2023), Unión Europea (2024), OCDE (2022) y MICITT (2024).

El análisis revela que, si bien existen marcos robustos y ampliamente reconocidos, ninguno de ellos fue diseñado específicamente para organizaciones con las características y limitaciones de las Pymes costarricenses. El NIST AI RMF destaca por su flexibilidad y escalabilidad, lo que lo convierte en la referencia estructural más adecuada para la propuesta. La ISO/IEC 42001 aporta un modelo de gestión formal, aunque su complejidad requiere una simplificación significativa. El AI Act ofrece principios regulatorios valiosos, pero su orientación hacia proveedores de sistemas de alto riesgo limita su aplicabilidad directa. Los principios de la OCDE y la ENIA-CR proveen el marco ético y de política pública necesario para contextualizar la propuesta en el ámbito nacional.

2.6 Relación de conceptos

La gobernanza de la inteligencia artificial se articula con la gestión del riesgo, la ética y la estructura organizacional de las Pymes. Esta interrelación puede representarse como un sistema en el que la ética define los principios, la gestión del riesgo operacionaliza los controles y la gobernanza integra ambos dentro de la estrategia empresarial, adaptándose al contexto y las capacidades de cada organización.

En conjunto, estos elementos proporcionan la base conceptual que orienta la propuesta aplicada de esta investigación, cuyo diseño se detalla en el Capítulo 5.

Capítulo 3. Marco Metodológico

El presente capítulo describe el enfoque metodológico adoptado para desarrollar esta investigación aplicada, la cual busca diseñar una propuesta de marco de gobernanza de inteligencia artificial adaptado a las Pymes costarricenses. Se detallan el tipo de investigación, su alcance, el enfoque utilizado, el diseño, la población de referencia y el proceso de muestreo teórico empleado para la selección de fuentes.

3.1 Tipo de investigación

Esta investigación es de tipo aplicado, ya que su propósito principal es la creación de un modelo práctico de gobernanza de IA basado en la adaptación de marcos internacionales a la realidad de las Pymes costarricenses. A diferencia de la investigación puramente teórica, este estudio busca generar un resultado tangible que pueda implementarse y evaluarse en entornos organizacionales reales.

3.2 Alcance investigativo

El alcance de esta investigación es descriptivo y propositivo. Es descriptivo porque analiza el estado actual de la gobernanza de IA en los distintos marcos internacionales y contextualiza su situación en el entorno nacional.

Es propositivo porque, a partir de esa revisión, se plantea un modelo de gobernanza que integra componentes éticos, técnicos y normativos aplicables a Pymes.

3.3 Enfoque

El enfoque adoptado es cualitativo, sustentado en el análisis interpretativo de información documental y en la revisión sistemática de literatura especializada. Este enfoque

permite comprender los fenómenos de gobernanza y ética en IA desde una perspectiva contextual y no meramente estadística, priorizando la profundidad analítica sobre la cantidad de datos.

3.4 Diseño de la investigación

El diseño es no experimental y documental.

No experimental porque no se manipulan variables, sino que se analizan fenómenos en su contexto natural.

Documental porque se fundamenta en la recopilación, organización y análisis de fuentes secundarias como normas técnicas, marcos regulatorios, estudios académicos y políticas nacionales.

El diseño se orienta a generar una propuesta integradora que se valide mediante la coherencia teórica y la aplicabilidad práctica de los resultados.

3.5 Población y muestreo

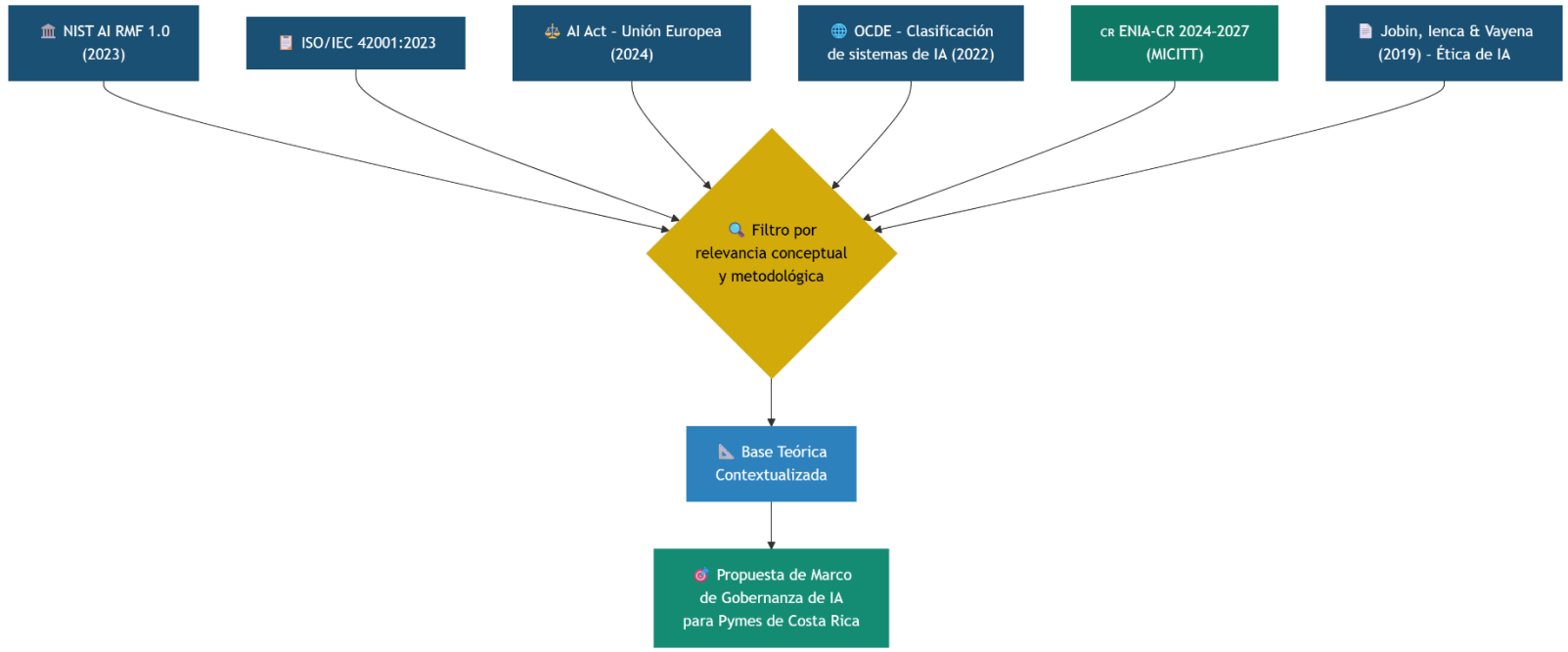
La población de referencia corresponde a las pequeñas y medianas empresas (Pymes) de Costa Rica, que constituyen más del 95% del tejido empresarial y desempeñan un papel clave en la economía nacional.

Fuente: Ministerio de Economía, Industria y Comercio (MEIC)

Figura 1. Proporción de Pymes en el tejido empresarial de Costa Rica.

Composición del tejido empresarial costarricense. Fuente: Elaboración propia con datos del MEIC.

El muestreo es no probabilístico de tipo teórico, ya que las fuentes y marcos seleccionados (NIST, ISO, Unión Europea, MICITT, entre otros) se eligieron con base en su relevancia conceptual y metodológica, más que en criterios estadísticos. Este enfoque permite construir una base teórica sólida y contextualizada que sirva de sustento a la propuesta aplicada.



3.6 Técnicas de análisis

Se emplea el análisis de contenido como técnica principal, mediante el cual se extraen categorías y variables comunes entre los marcos revisados como lo son sus roles, políticas, la gestión de riesgos, la ética y el cumplimiento. Estas categorías serán la base para estructurar el modelo de gobernanza propuesto.

Además, se utiliza la triangulación conceptual, comparando las fuentes internacionales con el contexto costarricense, con el fin de garantizar la pertinencia y aplicabilidad del modelo resultante.

3.7 Consideraciones éticas

Si bien la investigación es documental, se mantiene el compromiso ético de citar y referenciar correctamente todas las fuentes utilizadas, respetando los derechos de autor y la integridad académica. Además, el modelo propuesto promueve principios éticos en la gestión de inteligencia artificial, contribuyendo a su uso responsable dentro de las organizaciones.

4.0 Análisis de la situación

El análisis de la situación tiene como objetivo comprender el contexto actual en el que se encuentran las pequeñas y medianas empresas (Pymes) costarricenses respecto al uso y la gobernanza de la inteligencia artificial (IA). A partir de la revisión sistemática realizada y de la interpretación de los marcos internacionales consultados, se identificaron factores clave que influyen directa o indirectamente en la capacidad de las Pymes para adoptar sistemas de IA de manera ética, segura y alineada con las mejores prácticas.

Un primer aspecto identificado es que el nivel de madurez digital de las Pymes costarricenses continúa siendo limitado. Según datos del Ministerio de Economía, Industria y Comercio (MEIC), las micro, pequeñas y medianas empresas representan la amplia mayoría del tejido empresarial del país; no obstante, el diagnóstico incluido en la Estrategia Nacional de Inteligencia Artificial 2024–2027 (ENIA-CR) señala que gran parte de estas organizaciones no han incorporado prácticas formales de gestión tecnológica ni procesos estructurados de transformación digital (MICITT, 2024). Aunque muchas empresas han comenzado a incorporar herramientas basadas en IA, especialmente en áreas como mercadeo digital, automatización de procesos y análisis de datos, estas implementaciones se realizan frecuentemente sin estructuras formales de gobernanza tecnológica. La mayoría carece de políticas de uso de IA, controles de calidad de datos, procesos de documentación o lineamientos de gestión del riesgo algorítmico.

Por otra parte, se identificó que el país aún no cuenta con regulaciones específicas dirigidas al uso empresarial de la inteligencia artificial. La Estrategia Nacional de Inteligencia Artificial 2024–2027 (ENIA-CR) constituye un punto de partida importante, pero no provee directrices operativas para las Pymes, ni establece mecanismos claros de supervisión o cumplimiento. En ausencia de normativa especializada en IA, el principal instrumento legal aplicable es la Ley n.º 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, administrada por la Agencia de Protección de Datos de los Habitantes (PRODHAB). Esta ley establece obligaciones sobre el consentimiento informado, la finalidad del tratamiento, la seguridad de los datos y los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO). La adopción de herramientas de IA sin una gobernanza adecuada puede exponer a las Pymes al incumplimiento de esta normativa, particularmente cuando se procesan datos personales o sensibles en plataformas de terceros sin garantías claras de

privacidad, almacenamiento o tratamiento de la información. Este vacío normativo en materia de IA obliga a las empresas a depender de estándares internacionales como el Marco de Gestión de Riesgos de Inteligencia Artificial del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST AI RMF, por sus siglas en inglés) o la norma ISO/IEC 42001 para sistemas de gestión de inteligencia artificial. Sin embargo, estos marcos presentan barreras significativas para las Pymes, tanto por su alta carga documental y burocrática como por los costos asociados a procesos de certificación y auditoría, lo que refuerza la necesidad de contar con una guía simplificada y proporcional al contexto empresarial costarricense.

Asimismo, se encuentra una brecha significativa en la integración de principios éticos dentro de los procesos empresariales. Aunque los marcos internacionales destacan la importancia de la transparencia, la equidad, la rendición de cuentas y la mitigación de sesgos, la mayoría de las Pymes no cuenta con metodologías para evaluar estos aspectos en sus sistemas de IA. Esto representa un riesgo reputacional y operativo, especialmente en sectores que procesan datos personales o sensibles.

Finalmente, el ecosistema Pyme enfrenta limitaciones relacionadas con el acceso a talento especializado. La adopción de IA requiere conocimientos en ciencia de datos, ciberseguridad, análisis de riesgo y gobernanza tecnológica, pero la mayoría de las empresas no cuenta con estos perfiles profesionales. Esta brecha se explica tanto por la insuficiente oferta académica especializada en gobernanza de IA en el país, como por la incapacidad financiera de las Pymes para competir salarialmente con las empresas transnacionales establecidas en zonas francas y centros de servicios compartidos, lo que genera una migración de talento calificado hacia organizaciones de mayor escala. Como resultado, las Pymes enfrentan una doble desventaja: escasez de profesionales formados en estas disciplinas y dificultad para retener a quienes adquieren dichas competencias.

A partir de este análisis, se concluye que el contexto actual presenta una combinación de interés creciente en la IA, limitada capacidad de implementación responsable y ausencia de guías locales. Esto justifica la necesidad de un marco de gobernanza adaptado específicamente a las Pymes costarricenses, proporcional a sus recursos y alineado con los estándares internacionales.

5.0 Propuesta de marco de gobernanza de inteligencia artificial para Pymes

5.1 Propósito del marco

Este capítulo tiene como finalidad diseñar un marco de gobernanza de inteligencia artificial orientado a las pequeñas y medianas empresas costarricenses, particularmente aquellas pertenecientes a los sectores de servicios y comercio. Este marco busca ofrecer una estructura práctica y proporcional que permita a las organizaciones incorporar herramientas de inteligencia artificial de forma ética, segura y alineada con buenas prácticas internacionales.

La necesidad de este marco surge de la ausencia de lineamientos específicos para Pymes en Costa Rica, así como de la complejidad de los modelos internacionales existentes, los cuales suelen estar dirigidos a organizaciones con mayores recursos técnicos, financieros y humanos. En este sentido, la propuesta pretende funcionar como una guía adaptable que facilite la gestión responsable del uso de plataformas de IA, especialmente aquellas adquiridas como servicios de terceros o utilizadas para automatización, análisis de información y apoyo a la toma de decisiones.

El marco no pretende sustituir normas o regulaciones existentes, sino traducir sus principios a una realidad empresarial más accesible. Por ello, integra elementos de gestión del riesgo, ética digital, protección de datos, rendición de cuentas y mejora continua, con el propósito de fortalecer la confianza, la seguridad digital y la madurez organizacional de las Pymes costarricenses frente al uso de inteligencia artificial.

5.2 Principios rectores del marco

La propuesta de marco de gobernanza de inteligencia artificial se sustenta en un conjunto de principios rectores que orientan su diseño y futura aplicación en las Pymes costarricenses. Estos principios permiten alinear la adopción de inteligencia artificial con estándares internacionales, al tiempo que responden a la realidad operativa y organizacional del sector Pyme.

Transparencia.
El uso de sistemas de inteligencia artificial debe ser comprensible para la organización y, en la medida de lo posible, para las personas afectadas por sus resultados. Las Pymes deben procurar que las decisiones asistidas por IA puedan ser explicadas de forma clara y documentada, especialmente en procesos que impacten a clientes, empleados o decisiones organizacionales relevantes. Asimismo, se recomienda evitar el uso de datos sensibles en

plataformas de inteligencia artificial, salvo que existan controles adecuados de protección y cumplimiento normativo.

Responsabilidad.
Toda implementación de inteligencia artificial debe tener responsables definidos dentro de la organización. Este principio implica que el uso de IA no puede considerarse un proceso autónomo o sin supervisión, sino una actividad bajo control institucional.

Ética.
La incorporación de IA debe respetar principios de equidad, no discriminación y uso responsable de la información. El marco reconoce que las Pymes también deben considerar los impactos éticos de estas tecnologías, aunque operen a menor escala.

Seguridad.
La protección de la información utilizada, procesada o generada por sistemas de IA constituye un principio fundamental. Las organizaciones deben establecer controles mínimos para reducir riesgos como filtración de datos, accesos no autorizados, uso indebido de plataformas o dependencia insegura de proveedores externos.

Protección de datos.
El marco incorpora la necesidad de que las Pymes gestionen la información conforme a principios de privacidad y tratamiento adecuado de datos personales, en concordancia con la normativa costarricense vigente, particularmente con la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.

En este sentido, las organizaciones deben establecer criterios claros para determinar qué tipo de información puede ser utilizada en sistemas de inteligencia artificial, evitando prácticas que puedan comprometer la privacidad de clientes, empleados o terceros.

Se recomienda que las Pymes eviten procesar datos personales sensibles en plataformas de inteligencia artificial de terceros, especialmente cuando no existan garantías claras de privacidad, almacenamiento o tratamiento de la información. Esta práctica reduce significativamente el riesgo de exposición de datos, incumplimiento normativo y posibles impactos reputacionales para la organización.

Proporcionalidad.
El nivel de gobernanza aplicado debe ser coherente con el tamaño, recursos y nivel de

exposición al riesgo de cada Pyme. Este principio permite que el marco sea realista, flexible y escalable, evitando imponer cargas excesivas a organizaciones con capacidades limitadas.

Mejora continua.
La gobernanza de IA no debe entenderse como una acción única, sino como un proceso de revisión y ajuste permanente. Las Pymes deberán evaluar periódicamente sus prácticas, riesgos y controles para adaptarse a los cambios tecnológicos y normativos.

5.3 Estructura del marco de gobernanza de inteligencia artificial

El marco de gobernanza de inteligencia artificial propuesto en esta investigación se estructura a partir de un enfoque modular que integra componentes organizacionales, técnicos y éticos. Esta estructura busca facilitar la adopción progresiva de prácticas de gobernanza dentro de las pequeñas y medianas empresas (Pymes) costarricenses, considerando sus limitaciones de recursos y su nivel de madurez digital.

El diseño del marco toma como referencia buenas prácticas internacionales, particularmente el Artificial Intelligence Risk Management Framework (NIST, 2023), la norma ISO/IEC 42001:2023 para sistemas de gestión de inteligencia artificial, y los principios éticos promovidos por organismos internacionales como la OCDE y la Unión Europea. No obstante, la propuesta adapta estos lineamientos a un modelo simplificado que pueda ser aplicado de manera práctica por organizaciones de menor escala.

5.3.1 Trazabilidad con marcos internacionales

Con el propósito de garantizar la fundamentación y rigurosidad del marco propuesto, la siguiente tabla presenta la relación entre cada componente del modelo de gobernanza y los marcos internacionales de los cuales se derivan sus elementos constitutivos. Esta trazabilidad permite evidenciar el proceso de adaptación realizado para ajustar lineamientos diseñados para organizaciones de mayor escala a la realidad operativa de las Pymes costarricenses.

El marco se compone de cinco componentes fundamentales, los cuales interactúan entre sí para garantizar una gobernanza integral del uso de la inteligencia artificial dentro de las Pymes.

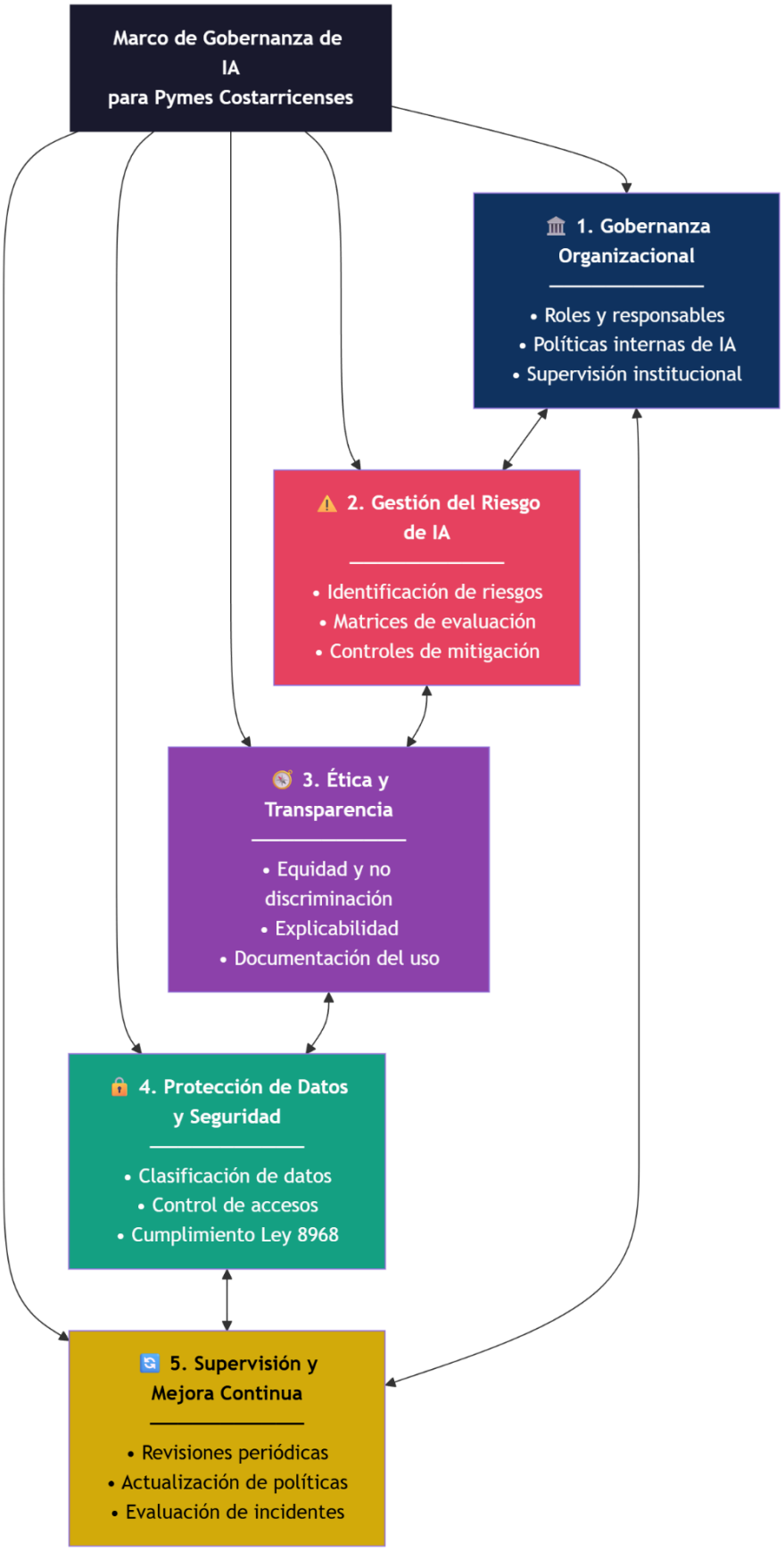
Trazabilidad del marco de gobernanza con marcos internacionales

Relación entre los componentes del modelo propuesto y sus fuentes de referencia

Componente del marco	NIST AI RMF 1.0	ISO ISO/IEC 42001	UE AI Act	OCDE Principios	CR ENIA-CR
1 **Gobernanza organizacional**	Función **GOVERN**: cultura organizacional, roles, rendición de cuentas	Cláusulas **5** (Liderazgo) y **6** (Planificación)	Arts. **9** y **17**: sistema de gestión de riesgos y calidad	Principio de rendición de cuentas	Eje de gobernanza y talento humano
2 **Gestión del riesgo de IA**	Funciones **MAP**, **MEASURE** y **MANAGE**: identificar, medir y mitigar riesgos	Cláusula **6.1**: acciones para abordar riesgos; **Anexo A**: controles	Arts. **6–7**: clasificación por niveles de riesgo	Marco de clasificación de sistemas de IA según riesgo	Eje de uso responsable y seguridad digital
3 **Ética y transparencia**	**GOVERN 1.x**: valores y principios organizacionales	Cláusula **5.2**: política de IA alineada con valores	Arts. **13–14**: transparencia y provisión de información	Principios de transparencia, explicabilidad y equidad	Eje de ética e inclusión
4 **Protección de datos y seguridad**	**MANAGE 2.x**: gestión de riesgos de privacidad	Cláusula **8**: operación; **Anexo A**: controles de seguridad	Arts. **10** y **15**: gobernanza de datos y ciberseguridad	Principio de seguridad y protección	Alineación con Ley 8968
5 **Supervisión y mejora continua**	**GOVERN 5.x**: monitoreo continuo	Cláusulas **9** (Evaluación) y **10** (Mejora)	Art. **61**: monitoreo posterior a la comercialización	Principio de robustez y evolución	Eje de seguimiento y evaluación

Fuente: Elaboración propia a partir de NIST (2023), ISO/IEC (2023), Unión Europea (2024), OCDE (2022) y MICITT (2024).

Tabla 1. Trazabilidad del marco de gobernanza propuesto con marcos internacionales de referencia.


Marco de Gobernanza de IA para Pymes Costarricenses
🏛️ 1. Gobernanza Organizacional
• Roles y responsables
• Políticas internas de IA
• Supervisión institucional
⚠️ 2. Gestión del Riesgo de IA
• Identificación de riesgos
• Matrices de evaluación
• Controles de mitigación
🧭 3. Ética y Transparencia
• Equidad y no discriminación
• Explicabilidad
• Documentación del uso
🔒 4. Protección de Datos y Seguridad
• Clasificación de datos
• Control de accesos
• Cumplimiento Ley 8968
🔄 5. Supervisión y Mejora Continua
• Revisiones periódicas
• Actualización de políticas
• Evaluación de incidentes

1. Gobernanza organizacional

Este componente establece la estructura de supervisión y toma de decisiones relacionadas con el uso de inteligencia artificial dentro de la organización. Su propósito es asegurar que la adopción de tecnologías de IA esté alineada con los objetivos estratégicos de la empresa, así como con principios éticos, legales y de seguridad.

Dentro de este componente se incluyen elementos como la definición de responsables del uso de herramientas de inteligencia artificial, la elaboración de políticas internas de uso de IA y la supervisión de su aplicación dentro de los procesos organizacionales.

En el contexto de las Pymes, la gobernanza organizacional no necesariamente implica la creación de estructuras complejas, sino la asignación clara de responsabilidades dentro de los roles existentes, permitiendo así mantener control institucional sobre el uso de estas tecnologías.

2. Gestión del riesgo de inteligencia artificial

La gestión del riesgo constituye uno de los pilares centrales del marco propuesto. Este componente se orienta a identificar, evaluar y mitigar los riesgos asociados al uso de sistemas de inteligencia artificial dentro de la organización.

Entre los principales riesgos considerados se encuentran:

- exposición de datos sensibles
- decisiones automatizadas con sesgos algorítmicos
- dependencia excesiva de proveedores externos de IA
- errores en resultados generados por modelos automatizados
- uso no autorizado de herramientas de inteligencia artificial por parte de empleados

La evaluación de estos riesgos puede realizarse mediante mecanismos simples como listas de verificación, análisis de impacto o matrices de riesgo, adaptadas a la realidad operativa de las Pymes.

Este enfoque permite incorporar prácticas de gestión del riesgo sin requerir estructuras complejas de cumplimiento o auditoría.

3. Ética y transparencia en el uso de IA

El tercer componente del marco aborda la dimensión ética del uso de la inteligencia artificial. Su propósito es garantizar que los sistemas utilizados por la organización respeten principios fundamentales como la equidad, la transparencia, la responsabilidad y el respeto por los derechos de las personas.

Las Pymes deben promover prácticas que permitan comprender cómo se utilizan las herramientas de IA dentro de la organización, especialmente cuando estas intervienen en procesos que afectan a clientes, empleados o decisiones empresariales relevantes.

Este componente también fomenta la documentación básica del uso de herramientas de inteligencia artificial, permitiendo que la organización tenga visibilidad sobre qué sistemas se utilizan, con qué propósito y bajo qué criterios.

La incorporación de principios éticos dentro de la gobernanza tecnológica contribuye a fortalecer la confianza organizacional y a reducir riesgos reputacionales.

4. Protección de datos y seguridad de la información

La protección de la información constituye un componente fundamental dentro del marco de gobernanza propuesto. La adopción de inteligencia artificial puede implicar el procesamiento de grandes volúmenes de datos, lo que incrementa la exposición a incidentes de seguridad y vulneraciones de privacidad.

En este contexto, las Pymes deben establecer controles básicos de seguridad orientados a proteger la confidencialidad, integridad y disponibilidad de la información utilizada por sistemas de inteligencia artificial.

Este componente contempla prácticas como:

- clasificación de la información utilizada por herramientas de IA
- restricción del uso de datos sensibles en plataformas externas
- control de accesos a herramientas de inteligencia artificial
- revisión de las políticas de privacidad de proveedores tecnológicos

Estas medidas permiten reducir riesgos de filtración de información, uso indebido de datos o incumplimiento normativo.

5. Supervisión y mejora continua

El último componente del marco se orienta a garantizar que la gobernanza de inteligencia artificial sea un proceso dinámico y evolutivo dentro de la organización.

Dado que las tecnologías de IA evolucionan rápidamente, las políticas y controles definidos por la empresa deben ser revisados periódicamente para asegurar su pertinencia y eficacia.

La supervisión puede realizarse mediante revisiones periódicas del uso de herramientas de inteligencia artificial, evaluación de incidentes relacionados con IA o actualización de las políticas internas conforme a cambios regulatorios o tecnológicos.

La incorporación de procesos de mejora continua permite que el marco de gobernanza se mantenga vigente y adaptado a la evolución del entorno digital.

5.4 Modelo de madurez progresivo de gobernanza de IA

El modelo de madurez propuesto permite a las Pymes evaluar su nivel actual de gobernanza de inteligencia artificial y avanzar de manera progresiva hacia prácticas más sólidas y estructuradas. Este modelo se organiza en cuatro niveles, diseñados para reflejar la realidad de organizaciones con distintos grados de preparación tecnológica, organizacional y normativa.

Nivel 1 – Inicial

En este nivel, la organización no cuenta con políticas, procesos ni controles formalizados para el uso de inteligencia artificial. Las herramientas de IA se utilizan de manera informal, sin supervisión institucional, sin asignación de responsabilidades y sin consideración de los riesgos asociados. Este escenario es el más frecuente en Pymes que han adoptado herramientas de IA de forma reactiva o por iniciativa individual de sus empleados, sin una decisión organizacional estructurada.

Las características propias de este nivel incluyen el uso informal y no documentado de herramientas de IA, la ausencia de políticas ni lineamientos de uso definidos, la falta de un responsable designado para la gobernanza de IA, la inexistencia de procesos de identificación o evaluación de riesgos, y una potencial exposición a incidentes de seguridad y privacidad que la organización no ha detectado ni gestionado.

Nivel 2 - Básico

En este nivel, la organización ha comenzado a establecer políticas básicas y a definir responsabilidades en torno al uso de inteligencia artificial. Existe conciencia sobre los riesgos principales, aunque los controles todavía son incipientes y no siempre se aplican de manera consistente en todos los procesos de la organización.

Las características propias de este nivel incluyen la existencia de una política básica de uso de herramientas de IA, la designación informal de un responsable de gobernanza tecnológica, una identificación inicial de los principales riesgos asociados al uso de IA, una clasificación básica de la información utilizada por dichas herramientas, y el cumplimiento mínimo de los requisitos normativos aplicables, particularmente la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.

Nivel 3 - Intermedio

La organización cuenta con procesos formales de gestión del riesgo, controles documentados y mecanismos de supervisión periódica. Las prácticas de gobernanza se aplican de manera consistente y los empleados conocen sus responsabilidades frente al uso de inteligencia artificial dentro del entorno organizacional.

Las características propias de este nivel incluyen un marco de gobernanza de IA formalmente documentado, procesos establecidos de identificación, evaluación y mitigación de riesgos, control de acceso a herramientas de IA con gestión de identidades, revisiones periódicas del cumplimiento de las políticas internas, capacitación básica al personal sobre uso responsable de IA, y registros documentados del uso de herramientas de inteligencia artificial por proceso y área.

Nivel 4 - Avanzado

En este nivel, la gobernanza de IA está completamente integrada en la cultura organizacional. Existe un ciclo activo de mejora continua, los controles son revisados y actualizados de manera regular, y la organización es capaz de adaptarse a cambios normativos y tecnológicos de forma proactiva, sin esperar a que los incidentes ocurran.

Las características propias de este nivel incluyen una cultura organizacional de uso ético y responsable de IA, auditorías internas de gobernanza realizadas periódicamente,

mecanismos formales de reporte de incidentes relacionados con IA, evaluación y actualización continua del marco de gobernanza, integración de criterios éticos en todos los procesos que involucren inteligencia artificial, y alineación activa con estándares internacionales como el NIST AI RMF y la ISO/IEC 42001.

Se recomienda que las Pymes inicien la implementación en el nivel que corresponda a su situación actual, evaluada mediante el instrumento de autoevaluación descrito en la sección 5.6, y avancen de forma progresiva sin exigirse alcanzar el nivel 4 de manera inmediata. La transición entre niveles debe estar guiada por los resultados de la autoevaluación y la hoja de ruta de implementación presentada en la sección 5.7.

5.5 Matriz de riesgos asociados al uso de inteligencia artificial

La siguiente matriz presenta los principales riesgos identificados a lo largo de la investigación, asociados al uso de plataformas de inteligencia artificial en las Pymes costarricenses. Para cada riesgo se indica su nivel de probabilidad, su impacto potencial, el nivel de riesgo resultante y las medidas de mitigación recomendadas para su gestión.

La matriz utiliza los siguientes criterios de valoración:

- La probabilidad se clasifica como Alta (3), Media (2) o Baja (1).
- El impacto se clasifica como Alto (3), Medio (2) o Bajo (1).
- El nivel de riesgo resulta del producto entre probabilidad e impacto, con un rango de 1 a 9, donde los valores entre 7 y 9 corresponden a un riesgo crítico, los valores entre 4 y 6 corresponden a un riesgo moderado, y los valores entre 1 y 3 corresponden a un riesgo bajo.

N	Riesgo	Descripción	Probabilidad	Impacto	Nivel de Riesgo	Mitigación recomendada
1	**Filtración de datos sensibles**	Ingreso de información confidencial en plataformas de IA externas sin controles adecuados.	Alta (3)	Alto (3)	9 Crítico	Política de clasificación de datos; prohibición de uso de datos sensibles en plataformas sin garantías; auditorías periódicas.
2	**Uso no autorizado de IA (Shadow IT)**	Empleados que utilizan herramientas de IA	Alta (3)	Alto (3)	9 Crítico	Política de uso aceptable de IA; inventario de herramientas

		sin autorización de la organización.				autorizadas; capacitación del personal.
3	**Sesgo algorítmico en decisiones organizacionales**	Resultados con sesgos que afectan negativamente a clientes, empleados u otros grupos.	Media (2)	Alto (3)	6 Moderado	Supervisión humana de decisiones críticas asistidas por IA; evaluación de las herramientas antes de su adopción.
4	**Dependencia excesiva de proveedores externos**	Riesgo de interrupción, cambios en condiciones o descontinuación de plataformas de IA utilizadas.	Alta (3)	Medio (2)	6 Moderado	Revisión de contratos con proveedores; plan de contingencia; diversificación de herramientas cuando sea posible.
5	**Incumplimiento normativo**	Uso de herramientas de IA en contradicción con la Ley 8968, ENIA-CR u otras normativas aplicables.	Media (2)	Alto (3)	6 Moderado	Revisión legal de las herramientas utilizadas; alineación con ENIA-CR; consulta con asesoría legal cuando sea necesario.
6	**Pérdida de integridad de la información**	Resultados incorrectos o alucinaciones generados por IA utilizados sin verificación humana.	Media (2)	Alto (3)	6 Moderado	Procesos de validación humana de resultados; no usar IA como fuente única en decisiones de impacto.
7	**Vulnerabilidades de seguridad en plataformas de terceros**	Fallos de seguridad en sistemas del proveedor que expongan datos de la organización.	Baja (1)	Alto (3)	3 Bajo	Revisión de políticas de privacidad del proveedor antes de la adopción; preferir plataformas con certificaciones reconocidas.
8	**Falta de documentación del uso de IA**	Imposibilidad de auditar o rendir cuentas sobre el uso de herramientas de IA por ausencia de registros.	Alta (3)	Medio (2)	6 Moderado	Registro de herramientas en uso; documentación del propósito, responsable y alcance de cada herramienta. Nota. La probabilidad y el impacto se valoran en escala 1-3 (Baja/Bajo=1, Media/Medio=2, Alta/Alto=3). El nivel

		de riesgo resulta del producto de ambos factores.

Esta matriz debe ser revisada y actualizada periódicamente, especialmente cuando se incorporen nuevas herramientas de inteligencia artificial a los procesos organizacionales o cuando ocurran cambios normativos relevantes en el entorno nacional o internacional.

5.6 Lista de chequeo de autoevaluación de gobernanza de IA

El presente instrumento permite a las Pymes evaluar de manera rápida y estructurada el nivel de cumplimiento de su gobernanza de inteligencia artificial, en relación con los cinco componentes del marco propuesto. Cada pregunta debe ser respondida con una de las siguientes opciones: Sí, En proceso o No, de acuerdo con el estado actual de la organización al momento de la evaluación.

Componente 1: Gobernanza organizacional

1. ¿Existe un responsable designado para la supervisión del uso de herramientas de IA en la organización?

2. ¿Se cuenta con una política interna de uso aceptable de inteligencia artificial?

3. ¿Los empleados que utilizan herramientas de IA conocen sus responsabilidades y los límites establecidos por la organización?

4. ¿Se lleva un inventario actualizado de las herramientas de IA utilizadas en la organización?

5. ¿Las políticas de uso de IA han sido comunicadas formalmente a todo el personal relevante?

Componente 2: Gestión del riesgo de inteligencia artificial

6. ¿Se ha realizado una identificación de los riesgos asociados al uso de herramientas de IA en la organización?

7. ¿Existe una matriz de riesgos o instrumento equivalente que documente los riesgos identificados y sus controles?

8. ¿Se han implementado controles concretos para mitigar los riesgos de mayor criticidad?

9. ¿La matriz de riesgos y los controles asociados son revisados y actualizados periódicamente?

10. ¿Los incidentes relacionados con el uso de IA son documentados y analizados para prevenir su recurrencia?

Componente 3: Ética y transparencia

11. ¿Las decisiones asistidas por IA que impactan a clientes o empleados pueden ser explicadas o justificadas por un responsable de la organización?

12. ¿Se evita el uso de herramientas de IA en procesos donde los resultados no puedan ser verificados o validados por una persona?

13. ¿Existe un mecanismo para reportar o cuestionar decisiones que parezcan incorrectas, injustas o sesgadas?

14. ¿La organización ha considerado los posibles impactos éticos de las herramientas de IA que utiliza actualmente?

15. ¿Se documenta el propósito y el alcance de cada herramienta de IA utilizada dentro de la organización?

Componente 4: Protección de datos y seguridad de la información

16. ¿Existe una clasificación de la información que establezca cuáles datos pueden ingresarse en plataformas de IA externas?

17. ¿Está prohibido el ingreso de datos personales sensibles en herramientas de IA de terceros sin controles de privacidad adecuados?

18. ¿Se han revisado las políticas de privacidad y seguridad de los proveedores de IA actualmente utilizados?

19. ¿Existe control de acceso a las herramientas de IA dentro de la organización, con usuarios y permisos definidos?

20. ¿Se lleva un registro del tipo de información procesada mediante sistemas de IA en los distintos procesos de la organización?

Componente 5: Supervisión y mejora continua

21. ¿Se realizan revisiones periódicas del cumplimiento de las políticas de uso de IA establecidas?

22. ¿Existe un proceso para actualizar el marco de gobernanza ante cambios normativos o tecnológicos relevantes?

23. ¿Se evalúa regularmente si las herramientas de IA utilizadas continúan siendo adecuadas, seguras y pertinentes?

24. ¿El personal recibe capacitación periódica sobre uso responsable de inteligencia artificial?

25. ¿Se miden indicadores de efectividad de las prácticas de gobernanza implementadas?

Interpretación de resultados:

- De 20 a 25 respuestas "Sí": Nivel 4 — Optimizado.

- De 13 a 19 respuestas "Sí": Nivel 3 — Gestionado.

- De 6 a 12 respuestas "Sí": Nivel 2 — Definido.

- De 0 a 5 respuestas "Sí": Nivel 1 — Inicial.

Se recomienda aplicar este instrumento al inicio del proceso de implementación del marco y de forma anual, con el propósito de monitorear el avance hacia niveles superiores de madurez en la gobernanza de inteligencia artificial.

Con el fin de que la supervisión sea medible y objetiva, el marco propone un conjunto de indicadores clave de desempeño que permiten medir objetivamente el avance de la gobernanza de IA. Entre los indicadores sugeridos se encuentran: el porcentaje de empleados

capacitados en uso responsable de inteligencia artificial, el número de incidentes de sesgo, privacidad o uso indebido reportados por período, el porcentaje de herramientas de IA documentadas en el inventario organizacional, y la variación en el nivel de madurez según el instrumento de autoevaluación. Estos indicadores se desarrollan en detalle en la sección 5.9 del presente documento.

5.7 Guía de implementación

La hoja de ruta de implementación proporciona una guía orientativa para que las Pymes puedan incorporar progresivamente el marco de gobernanza de inteligencia artificial. Se organiza en tres fases consecutivas, con actividades específicas y resultados esperados en cada etapa, concebidas para organizaciones con recursos y capacidades limitadas.

Fase 1: Diagnóstico y sensibilización (meses 1 y 2)

El objetivo de esta fase es establecer una línea base del nivel de madurez actual y generar conciencia organizacional sobre la necesidad de contar con prácticas de gobernanza de IA.

Las actividades correspondientes a esta fase incluyen la aplicación del checklist de autoevaluación para determinar el nivel de madurez inicial de la organización, la identificación y documentación de las herramientas de IA actualmente en uso, la realización de una sesión de sensibilización con el equipo directivo y el personal clave sobre los riesgos del uso de IA sin gobernanza, la designación de un responsable de gobernanza de IA dentro de la organización, y la documentación inicial de los riesgos identificados.

Los resultados esperados al finalizar esta fase son un inventario de herramientas de IA en uso, la designación formal de un responsable de gobernanza, el nivel de madurez inicial identificado mediante el checklist, y el equipo directivo informado sobre los objetivos y alcance del marco.

Fase 2: Implementación de controles básicos (meses 3 al 5)

El objetivo de esta fase es establecer las políticas, controles y procesos fundamentales que componen el núcleo operativo del marco de gobernanza.

Las actividades correspondientes a esta fase incluyen el desarrollo y aprobación de la política de uso aceptable de inteligencia artificial, la implementación de la matriz de riesgos y el establecimiento de acciones concretas para los riesgos clasificados como críticos, la

implementación de controles de acceso a las herramientas de IA, la definición de la clasificación de la información y los criterios de uso con herramientas externas, la comunicación formal de las políticas a todo el personal, y la realización de sesiones de capacitación sobre uso responsable de herramientas de IA.

Los resultados esperados al finalizar esta fase son la política de uso de IA aprobada y comunicada a la organización, los controles de acceso implementados, la clasificación de la información definida, y el personal capacitado en los principios básicos de gobernanza de IA establecidos por el marco.

Fase 3: Seguimiento y mejora continua (mes 6 en adelante)

El objetivo de esta fase es establecer los mecanismos de revisión periódica y actualización del marco de gobernanza, consolidando el ciclo de mejora continua.

Las actividades correspondientes a esta fase incluyen la realización de una segunda aplicación del checklist de autoevaluación para medir el avance respecto a la línea base inicial, la revisión y actualización de la matriz de riesgos al menos una vez al año, el establecimiento de un proceso formal de reporte de incidentes relacionados con el uso de IA, la evaluación de nuevas herramientas de IA con base en criterios de seguridad, privacidad y ética antes de su adopción, y la actualización del marco de gobernanza ante cambios normativos o tecnológicos relevantes.

Los resultados esperados en esta fase son un mecanismo de mejora continua activo, indicadores de gobernanza monitoreados con regularidad, y un marco de gobernanza actualizado y vigente que se adapta al entorno tecnológico y normativo en evolución.

5.8 Recursos necesarios para la implementación

Una de las barreras más frecuentes para la adopción de marcos de gobernanza en las Pymes es la percepción de costos elevados. El presente marco ha sido diseñado bajo el principio de proporcionalidad, de modo que su implementación no requiere inversiones significativas en software especializado ni infraestructura tecnológica adicional, pudiendo gestionarse íntegramente con herramientas de ofimática comunes. En concordancia con lo establecido en la sección 5.2, los recursos descritos a continuación han sido identificados considerando las capacidades reales del sector Pyme costarricense, organizados en tres dimensiones principales: humana, técnica y económica.

Recursos humanos

La implementación del marco no requiere la contratación de personal especializado adicional. Se recomienda, sin embargo, la designación de un responsable interno de gobernanza de IA, quien puede asumir esta función como parte de su rol actual dentro de la organización. Las responsabilidades típicas asociadas a este rol incluyen supervisar el cumplimiento de la política de uso de IA, coordinar las revisiones periódicas del marco, actuar como punto de contacto ante incidentes relacionados con inteligencia artificial, y facilitar la capacitación interna del personal.

Adicionalmente, se requiere la participación del equipo directivo para la aprobación de políticas y la asignación de los recursos necesarios, así como la colaboración del personal operativo en la aplicación consistente de los controles establecidos.

Recursos técnicos

El marco de gobernanza propuesto no requiere infraestructura tecnológica especializada. Los recursos técnicos necesarios consisten principalmente en el acceso a herramientas de productividad estándar tales como procesadores de texto y hojas de cálculo para la documentación de políticas, registros y matrices, así como conectividad a internet para el acceso a fuentes normativas y la actualización del conocimiento del marco. Se recomienda también contar con una plataforma de gestión documental, ya sea en la nube o de carácter local, para el almacenamiento organizado de políticas, registros e inventarios de herramientas.

Recursos económicos

El costo de implementación del marco de gobernanza es principalmente el tiempo del responsable designado y del equipo directivo involucrado. No se requieren inversiones en software especializado, consultoría externa obligatoria ni infraestructura adicional. El costo estimado se asocia a las horas dedicadas a las siguientes actividades: el diagnóstico inicial y la aplicación del checklist de autoevaluación, con una duración estimada de entre cuatro y ocho horas; la elaboración de políticas y documentos, con una duración estimada de entre diez y dieciséis horas; las sesiones de sensibilización y capacitación al personal, con una duración estimada de entre dos y cuatro horas; y las revisiones periódicas anuales del marco, con una duración estimada de entre cuatro y seis horas por ciclo.

Esta estructura de costos hace que el marco sea accesible incluso para Pymes con presupuestos limitados, en plena concordancia con el principio de proporcionalidad que orienta toda la propuesta.

5.9 Criterios de evaluación del marco

Con el propósito de verificar la efectividad y vigencia del marco de gobernanza de inteligencia artificial a lo largo del tiempo, se establecen los siguientes criterios de evaluación. Estos criterios permiten a las organizaciones determinar si las prácticas implementadas están generando los resultados esperados y si el marco requiere ajustes o actualizaciones.

Criterio 1: Cobertura del inventario de herramientas de IA

Indicador: Porcentaje de herramientas de IA conocidas y en uso que se encuentran documentadas en el inventario organizacional.

Meta: 100% de las herramientas identificadas con documentación actualizada.

Frecuencia de evaluación: Semestral.

Criterio 2: Cumplimiento de la política de uso de IA

Indicador: Porcentaje de empleados que utilizan herramientas de IA y que han recibido y aceptado formalmente la política de uso aceptable.

Meta: 100% del personal usuario de herramientas de IA.

Frecuencia de evaluación: Anual.

Criterio 3: Reducción de riesgos críticos

Indicador: Número de riesgos clasificados como críticos en la matriz de riesgos que cuentan con al menos un control activo implementado.

Meta: 100% de los riesgos críticos con controles implementados y documentados.

Frecuencia de evaluación: Anual o ante cambios significativos en el entorno tecnológico o normativo.

Criterio 4: Avance en el nivel de madurez

Indicador: Variación en el puntaje del checklist de autoevaluación entre ciclos de evaluación consecutivos.

Meta: Avance de al menos un nivel de madurez cada 12 a 18 meses de implementación activa del marco.

Frecuencia de evaluación: Anual.

Criterio 5: Gestión de incidentes relacionados con IA

Indicador: Número de incidentes de seguridad, privacidad o uso indebido de inteligencia artificial documentados por período.

Meta: Tendencia sostenida de reducción de incidentes tras la implementación de los controles establecidos en el marco.

Frecuencia de evaluación: Trimestral.

Criterio 6: Capacitación del personal

Indicador: Porcentaje del personal que utiliza herramientas de IA y que ha recibido al menos una sesión de capacitación sobre uso responsable de inteligencia artificial.

Meta: 100% del personal usuario de herramientas de IA capacitado por ciclo anual.

Frecuencia de evaluación: Anual.

La evaluación de estos criterios debe ser documentada por el responsable de gobernanza de IA designado, y sus resultados deben utilizarse como insumo para la revisión y actualización del marco dentro del proceso de mejora continúa descrito en la sección 5.8.

5.10 Caso de uso: Pyme de servicios contables que utiliza ChatGPT

Con el propósito de ilustrar la aplicabilidad del marco de gobernanza propuesto, se presenta un caso hipotético basado en un escenario representativo del contexto Pyme costarricense. Este ejercicio permite visualizar cómo los cinco componentes del marco, junto con las herramientas de apoyo desarrolladas en las secciones anteriores, pueden ser implementados de forma progresiva en una organización real.

Descripción de la empresa

ContaDigital S.R.L. es una firma de servicios contables y asesoría tributaria con 32 empleados, ubicada en el Gran Área Metropolitana de Costa Rica. La empresa ofrece servicios de contabilidad general, preparación de declaraciones de impuestos y asesoría financiera a pequeñas empresas y personas físicas con actividad lucrativa. Hace aproximadamente seis meses, dos de sus colaboradores comenzaron a utilizar ChatGPT por iniciativa propia para asistir en la redacción de informes financieros, la generación de respuestas a consultas tributarias de clientes y el análisis preliminar de datos contables. La gerencia no tomó una decisión formal al respecto ni estableció lineamientos de uso.

Fase 1: Diagnóstico y sensibilización

El gerente general, al conocer publicaciones sobre los riesgos de la inteligencia artificial en el manejo de datos, decide aplicar el instrumento de autoevaluación descrito en la sección 5.6. El resultado es de 2 respuestas afirmativas de 25, lo que ubica a la empresa en el Nivel 1 Inicial del modelo de madurez (sección 5.4).

Las respuestas permiten identificar las siguientes condiciones:

Gobernanza organizacional: No existe un responsable designado para el uso de IA, no se cuenta con una política de uso, y no se lleva un inventario de herramientas. Los empleados desconocen qué límites aplican.

Gestión del riesgo: No se ha realizado ninguna identificación formal de riesgos asociados al uso de ChatGPT. No existe matriz de riesgos ni controles implementados.

Ética y transparencia: Los colaboradores utilizan ChatGPT para generar respuestas a clientes sin que estos lo sepan. No existe un mecanismo para reportar resultados incorrectos o sesgados. No se ha evaluado el impacto ético del uso de la herramienta.

Protección de datos: Se descubre que los colaboradores han ingresado datos sensibles de clientes, incluyendo números de cédula, estados financieros y detalle de obligaciones tributarias, directamente en la plataforma de ChatGPT. No se ha revisado la política de privacidad del proveedor. No existe clasificación de la información ni control de acceso a la herramienta. Esto representa un riesgo concreto de incumplimiento de la Ley n.º 8968 de Protección de Datos Personales.

Supervisión y mejora continua: No existe ningún proceso de revisión ni indicadores de seguimiento.

Fase 2: Implementación de controles básicos

A partir del diagnóstico, la gerencia designa al encargado de tecnología de la información como responsable de gobernanza de IA y procede a implementar las siguientes acciones conforme a las instrucciones descritas en la sección 5.7

Gobernanza organizacional: Se elabora y aprueba una política de uso aceptable de inteligencia artificial. La política establece que ChatGPT puede utilizarse como herramienta de apoyo, pero que todos los productos generados deben ser revisados por un profesional antes de entregarse al cliente.

Se realiza un inventario de herramientas de IA en uso, identificándose dos: ChatGPT (versión gratuita) y un complemento de Excel con funciones de análisis predictivo.

Se asignan roles conforme a la estructura de gobernanza organizacional del componente 1: el gerente general como responsable último, el encargado de TI como ejecutor, y los colaboradores usuarios como informados.

Gestión del riesgo: Se aplica la matriz de riesgos de la sección 5.5. Se identifican los siguientes riesgos con su valoración:

- Exposición de datos financieros sensibles de clientes en ChatGPT: probabilidad alta (3), impacto alto (3), nivel de riesgo 9 – crítico.
- Entrega de información tributaria incorrecta generada por IA sin verificación: probabilidad media (2), impacto alto (3), nivel de riesgo 6 – moderado.
- Uso no autorizado de ChatGPT por nuevos empleados sin conocimiento de la política: probabilidad media (2), impacto medio (2), nivel de riesgo 4 – moderado.

Para el riesgo crítico, se implementa como control inmediato la prohibición de ingresar datos personales o financieros reales en la plataforma. Se establece que los prompts deben utilizar datos anonimizados o ficticios como insumo.

Ética y transparencia: Se incorpora en la política de uso una cláusula que obliga a informar al cliente cuando un producto entregable ha sido asistido por herramientas de inteligencia artificial. Se establece un mecanismo interno para que los colaboradores reporten

casos en que ChatGPT haya generado información incorrecta, sesgada o no verificable. Se documenta el propósito y alcance de cada herramienta en el inventario de IA.

Protección de datos y seguridad: Se clasifica la información de la empresa en tres niveles: pública, interna y confidencial. Se establece que únicamente la información pública o interna, debidamente anonimizada, puede ser utilizada en plataformas de IA externas.

Se revisan las políticas de privacidad de OpenAI y se documenta que, en la versión gratuita, los datos ingresados pueden ser utilizados para entrenamiento del modelo, lo cual refuerza la necesidad de no ingresar información confidencial.

Se implementa control de acceso: solo los colaboradores autorizados por el responsable de gobernanza pueden utilizar ChatGPT en el contexto laboral.

Supervisión y mejora continua: Se define una revisión trimestral del cumplimiento de la política por parte del responsable de gobernanza. Se establecen los siguientes indicadores de desempeño conforme a la sección 5.9:

- Porcentaje de empleados capacitados: meta 100 %
- Número de incidentes de ingreso de datos sensibles: meta 0
- Porcentaje de herramientas documentadas: meta 100 %

Fase 3: Seguimiento y resultados

Seis meses después de la implementación, se aplica nuevamente la lista de autoevaluación. La empresa obtiene 14 respuestas afirmativas de 25, lo que la ubica en el Nivel 3 – Gestionado del modelo de madurez, habiendo avanzado dos niveles en el período.

Los indicadores de desempeño registran los siguientes resultados:

- Porcentaje de empleados capacitados en uso responsable de IA: 100 % (32 de 32 empleados completaron la sesión de capacitación).
- Incidentes de ingreso de datos sensibles en plataformas de IA: 0 incidentes desde la implementación de la política.
- Herramientas de IA documentadas en el inventario organizacional: 100 % (2 de 2 herramientas).

Variación en el nivel de madurez: avance de Nivel 1 a Nivel 3 en seis meses de implementación activa. Se programa una revisión a los 12 meses para evaluar la incorporación

de controles adicionales que permitan avanzar hacia el Nivel 4 – Optimizado, incluyendo auditorías internas y mecanismos formales de mejora continua.

Conclusión del caso Este caso práctico demuestra que una Pyme costarricense puede implementar el marco de gobernanza propuesto de forma progresiva, con recursos mínimos y sin requerir inversiones en software o infraestructura adicional. Las herramientas proporcionadas por el marco, la autoevaluación, la matriz de riesgos, la política de uso, los indicadores de desempeño y el modelo de madurez, funcionan de manera articulada para guiar a la organización desde un estado de uso informal hacia una gestión estructurada y responsable de la inteligencia artificial, reduciendo riesgos concretos de seguridad, privacidad y cumplimiento normativo.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

Las conclusiones que se presentan a continuación se generan directamente del cumplimiento de cada uno de los objetivos formulados para esta investigación, siguiendo las indicaciones metodológicas de la Taxonomía de Bloom adoptada como marco cognitivo del proyecto.

En relación con el primer objetivo específico identificar y analizar los principales marcos y modelos internacionales de gobernanza de inteligencia artificial, el análisis comparativo desarrollado sobre el NIST AI RMF (2023), la norma ISO/IEC 42001:2023 y el AI Act de la Unión Europea permitió concluir que, si bien estos marcos representan referentes sólidos y ampliamente reconocidos a nivel global, fueron diseñados principalmente para organizaciones con recursos técnicos, financieros y humanos significativos. Su aplicación directa en el contexto de las Pymes costarricenses resulta inviable sin una adaptación profunda y estructurada. De los tres marcos analizados, el NIST AI RMF ofrece la mayor flexibilidad y potencial de adaptación para organizaciones de menor escala, gracias a su estructura modular y su orientación basada en funciones. Esta conclusión sirvió como punto de partida para el diseño del marco propuesto en el capítulo cinco.

En relación con el segundo objetivo específico analizar los riesgos éticos, legales, técnicos y de seguridad de la información asociados a la adopción de inteligencia artificial en las Pymes de Costa Rica, se concluye que los riesgos de mayor criticidad identificados son la

filtración de datos sensibles mediante plataformas externas y el uso no autorizado de herramientas de IA por parte de empleados, fenómeno conocido como shadow IT. Ambos riesgos presentan alta probabilidad de ocurrencia y elevado impacto potencial, y se potencian significativamente en entornos donde no existen políticas de uso formalizadas, situación que caracteriza a la mayoría de las Pymes costarricenses. La ausencia de normativa específica aplicable al uso empresarial de la inteligencia artificial en Costa Rica agrava este panorama, dejando a las organizaciones sin referentes legales claros para orientar sus prácticas.

En relación con el tercer objetivo específico desarrollar el marco de gobernanza institucional que incluya políticas, lineamientos éticos y controles de seguridad para la realidad operativa de las Pymes, se concluye que el marco propuesto, estructurado en cinco componentes interrelacionados gobernanza organizacional, gestión del riesgo de inteligencia artificial, ética y transparencia, protección de datos y seguridad de la información, y supervisión y mejora continua, constituye una respuesta coherente y fundamentada a las necesidades identificadas en el análisis de la situación. Cada componente fue diseñado con criterios de proporcionalidad y progresividad, de modo que su implementación no exija inversiones desproporcionadas ni estructuras organizacionales complejas. La incorporación de herramientas prácticas modelo de madurez, matriz de riesgos, checklist de autoevaluación y hoja de ruta fortalece la aplicabilidad del marco en la realidad operativa de las Pymes y lo distingue de los marcos de referencia internacionales existentes.

En relación con el cuarto objetivo específico validar la pertinencia, viabilidad y aplicabilidad del marco mediante el juicio de expertos, se concluye que la validación prevista con profesionales en ciberseguridad, gobernanza tecnológica e inteligencia artificial constituye el mecanismo idóneo para confirmar la coherencia interna del marco y su adecuación al contexto de las Pymes costarricenses. Los criterios de evaluación propuestos en la sección 5.9 servirán como base para verificar, en una etapa posterior a este trabajo, que las prácticas implementadas generan los resultados esperados en términos de reducción de riesgos y mejora de la madurez organizacional en la gobernanza de la inteligencia artificial.

En relación con el objetivo general diseñar un marco de gobernanza para el uso responsable de plataformas de inteligencia artificial en las pequeñas y medianas empresas costarricenses, alineado con estándares internacionales y adaptado a sus capacidades técnicas, organizacionales y financieras, se concluye que el presente trabajo constituye un aporte relevante y pertinente para el ecosistema empresarial costarricense. El marco diseñado responde a un vacío real de gobernanza, es coherente con los principios y estándares

internacionales reconocidos, y fue construido con una orientación práctica y proporcional que lo distingue de los marcos de referencia existentes. Su implementación progresiva, guiada por el modelo de madurez y la hoja de ruta propuestos, ofrece a las Pymes un camino viable para adoptar la inteligencia artificial de forma ética, segura y alineada con los estándares globales vigentes.

Desde la perspectiva de la ciberseguridad, se concluye adicionalmente que el uso de herramientas de inteligencia artificial externas, como ChatGPT, Copilot o Gemini, opera bajo un modelo de responsabilidad compartida en el que el proveedor de la plataforma gestiona la seguridad de la infraestructura y del modelo, pero la organización usuaria es responsable de los datos que ingresa, de las decisiones que toma con base en los resultados obtenidos y de los controles que implementa para proteger la información de sus clientes y colaboradores. Esta corresponsabilidad es ampliamente ignorada por las Pymes costarricenses, que tienden a asumir que la seguridad es una responsabilidad exclusiva del proveedor tecnológico. El presente trabajo permite concluir que la gobernanza de inteligencia artificial no debe entenderse como un proceso administrativo o burocrático, sino como un control de seguridad crítico, equiparable en importancia a la gestión de accesos, las copias de respaldo o la protección perimetral. Sin gobernanza, el uso de IA constituye un vector de riesgo no gestionado dentro de la postura de seguridad de la organización. Asimismo, se concluye que la ausencia de gobernanza en el uso de inteligencia artificial representa una amenaza directa a la resiliencia operativa y la continuidad del negocio de las Pymes. Una Pyme que depende de herramientas de IA para procesos críticos, como la generación de informes, la atención al cliente o el análisis de datos financieros, sin haber evaluado los riesgos de interrupción del servicio, cambios unilaterales en las políticas del proveedor o alteraciones en la calidad de los resultados, se expone a una disrupción operativa ante la cual no dispone de planes de contingencia ni alternativas documentadas. La gobernanza de IA, en este sentido, cumple también una función de continuidad operativa al exigir que la organización identifique sus dependencias tecnológicas, evalúe escenarios de fallo y establezca mecanismos mínimos de respuesta.

6.2 Recomendaciones

A partir del proceso de investigación desarrollado, se formulan las siguientes recomendaciones orientadas tanto a mejorar la aplicabilidad del marco propuesto como a fortalecer las condiciones del entorno en el que este deberá implementarse.

Se recomienda que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y las instituciones de apoyo al sector Pyme, tales como el Ministerio de Economía, Industria y Comercio (MEIC) y PROCOMER, desarrollen materiales de divulgación y guías simplificadas basadas en marcos como el propuesto en esta investigación. Este tipo de recursos facilitaría que las organizaciones de menor capacidad técnica puedan acceder a lineamientos prácticos de gobernanza de IA de forma accesible y sin barreras económicas.

Se recomienda que futuras investigaciones desarrollen estudios de implementación piloto del marco propuesto en Pymes reales de distintos sectores, con el propósito de validar empíricamente su efectividad, identificar ajustes necesarios y generar evidencia cuantificable sobre su impacto en la reducción de riesgos y el mejoramiento del nivel de madurez organizacional en la gobernanza de inteligencia artificial.

Se recomienda que el marco sea revisado y actualizado al menos cada dos años, dado el dinamismo con el que evolucionan tanto las tecnologías de inteligencia artificial como los marcos regulatorios internacionales. La incorporación de mecanismos de actualización normativa dentro del componente de supervisión y mejora continua facilita esta tarea y reduce el riesgo de que el marco quede desactualizado frente a cambios relevantes en el entorno.

Se recomienda al programa académico de la Maestría en Ciberseguridad y Seguridad de la Información considerar la incorporación de la gobernanza de IA como temática dentro de sus contenidos, dado que esta representa una intersección crítica entre la seguridad de la información, la ética digital y la gestión organizacional, áreas de creciente relevancia para los profesionales del sector.

Se recomienda a las Pymes que utilizan herramientas de inteligencia artificial externas implementar controles técnicos preventivos orientados a reducir el riesgo de exfiltración involuntaria de datos sensibles. Entre las medidas aplicables se encuentra el uso de soluciones de prevención de pérdida de datos (DLP, por sus siglas en inglés), la configuración de extensiones de navegador gestionadas que restrinjan la acción de pegado de información en plataformas de IA externas, o la habilitación de listas de sitios permitidos en los navegadores corporativos. Estos controles no requieren inversiones significativas y pueden implementarse con herramientas de administración estándar disponibles en la mayoría de los sistemas operativos empresariales.

Se recomienda que, previo a la utilización de cualquier herramienta de inteligencia artificial para el análisis o procesamiento de información, las Pymes realicen un proceso básico de saneamiento de datos (data cleaning). Esta práctica consiste en verificar la integridad, consistencia y actualización de los datos que serán utilizados como insumo para los sistemas de IA, con el propósito de evitar que información errónea, duplicada, desactualizada o sesgada contamine los resultados generados por la herramienta y afecte la toma de decisiones organizacionales. El saneamiento de datos constituye una medida preventiva de bajo costo que fortalece tanto la calidad de los resultados como la confiabilidad del proceso de gobernanza.

Se recomienda que los programas de capacitación sobre uso responsable de inteligencia artificial incluyan un componente específico de formación en ingeniería de prompts segura (secure prompt engineering). Esta formación debe orientar a los colaboradores en técnicas para interactuar con plataformas de IA sin revelar información confidencial, secretos industriales ni datos personales de clientes. Entre las prácticas recomendadas se incluyen la anonimización de los datos antes de su inclusión en los prompts, la sustitución de nombres, cifras y datos identificables por valores ficticios representativos, y la verificación previa de que el contenido del prompt no contiene información clasificada como confidencial según la política de uso de IA de la organización. Este tipo de formación especializada complementa la capacitación general y fortalece la primera línea de defensa contra la exposición involuntaria de información sensible.

Se recomienda que las Pymes realicen revisiones periódicas para identificar el uso de herramientas de inteligencia artificial no aprobadas formalmente por la organización, práctica conocida como shadow AI. Esta revisión puede ejecutarse mediante la inspección de los registros de navegación en los equipos corporativos, la consulta directa a los equipos de trabajo o la aplicación de encuestas internas anónimas. La detección temprana de herramientas no autorizadas permite evaluar sus riesgos, decidir si deben ser incorporadas al inventario oficial bajo los controles establecidos en el marco de gobernanza, o si deben ser restringidas. El shadow AI representa uno de los vectores de riesgo más frecuentes en las Pymes y su gestión proactiva es esencial para mantener la integridad de la postura de seguridad de la organización.

Se recomienda a las Pymes con un nivel de madurez intermedio o avanzado en gobernanza de IA evaluar la implementación de soluciones de proxy o gateway de inteligencia artificial que permitan centralizar, auditar y controlar el tráfico de información entre los usuarios de la organización y las plataformas de IA externas. Estas soluciones actúan como

intermediarios técnicos que registran los prompts enviados, aplican reglas de filtrado para bloquear el envío de datos sensibles y generan registros de auditoría que facilitan la supervisión y el cumplimiento normativo. El Anexo A del presente documento desarrolla esta recomendación con mayor detalle técnico para orientar su implementación práctica.

Finalmente, se recomienda a las Pymes costarricenses no postergar la implementación de prácticas básicas de gobernanza de inteligencia artificial en espera de regulaciones nacionales específicas. Las herramientas proporcionadas en este marco, especialmente el checklist de autoevaluación y la hoja de ruta, permiten iniciar un proceso de mejora gradual con los recursos disponibles, reduciendo de forma significativa la exposición a riesgos de seguridad, privacidad y cumplimiento normativo desde las etapas más tempranas de la adopción de inteligencia artificial.

Bibliografía

Microsoft. (2025, mayo 12). *50 % de las pymes en Costa Rica utilizan algún tipo de IA, según encuesta*. Microsoft News Center Latinoamérica. https://news.microsoft.com/es-xl/50-de-las-pymes-en-costa-rica-utilizan-algun-tipo-de-ia

MICITT. (2024). *Estrategia Nacional de Inteligencia Artificial de Costa Rica 2024-2027*. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. https://www.camtic.org/wp-content/uploads/2024/04/Estrategia-Nacional-de-Inteligencia-Artificial-Version-21.03.24-Para-consulta-pu%CC%81blica.pdf

Unión Europea. (2023). *Proposal for an Artificial Intelligence Act*. European Commission.

Organización Internacional de Normalización. (2023). *ISO/IEC 42001:2023 – Information technology - Artificial intelligence - Management system*. ISO.

Instituto Nacional de Estándares y Tecnología. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Biolchini, J., Gomes, P., Cruz, A., & Horta, F. (2005). *Systematic Review in Software Engineering*. Technical Report RT-ES 679/05. COPPE/UFRJ.

Organización para la Cooperación y el Desarrollo Económico. (2022). *OECD Framework for the Classification of AI Systems.* OCDE.

Ray, S. (2023, mayo 2). Samsung bans ChatGPT among employees after sensitive code leak. *Forbes*. https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399. https://www.nature.com/articles/s42256-019-0088-2

Bloom, B. S. (Ed.). (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Longmans, Green.

Anexos

Anexo A. Gateways de inteligencia artificial como control técnico de gobernanza

A.1 Propósito del anexo

El presente anexo tiene como propósito orientar a los encargados de tecnología de información y seguridad de las Pymes costarricenses sobre la implementación de gateways o proxies de inteligencia artificial como mecanismo técnico de soporte a la gobernanza de IA. Mientras que el marco propuesto en el capítulo cinco establece los componentes organizacionales, éticos y de gestión del riesgo, este anexo aborda la capa de infraestructura técnica que permite hacer cumplir las políticas definidas de manera automatizada, reduciendo la dependencia exclusiva del cumplimiento voluntario por parte de los colaboradores.

A.2 Concepto de gateway de inteligencia artificial

Un gateway de IA es una solución técnica que se ubica entre los usuarios de la organización y las plataformas de inteligencia artificial externas (como ChatGPT, Gemini, Copilot u otras). Funciona de manera análoga a un proxy web o un firewall de aplicaciones: intercepta las solicitudes salientes, aplica reglas predefinidas y registra la actividad para fines de auditoría.

Sus funciones principales incluyen:

- Inspección de contenido saliente: analiza los prompts enviados por los usuarios antes de que lleguen a la plataforma de IA, detectando patrones que correspondan a datos sensibles como números de cédula, información financiera, nombres de clientes o datos clasificados como confidenciales según la política de uso de la organización.
- Bloqueo o redacción automática: cuando se detecta información sensible, el gateway puede bloquear el envío del prompt, redactar (enmascarar) los datos sensibles antes de transmitirlos, o alertar al usuario y al responsable de gobernanza.
- Registro de auditoría: genera un log centralizado de todos los prompts enviados y las respuestas recibidas, lo que permite realizar revisiones periódicas, investigar incidentes y demostrar cumplimiento normativo ante la PRODHAB u otros entes de supervisión.

- Control de acceso por plataforma: permite definir qué herramientas de IA están autorizadas y bloquear el acceso a plataformas no aprobadas, contribuyendo a la gestión del shadow AI.

A.3 Opciones de implementación según la capacidad de la Pyme

La implementación de un gateway de IA no requiere necesariamente inversiones elevadas. Existen distintas alternativas que se adaptan a los diferentes niveles de madurez y presupuesto:

Nivel básico (costo mínimo): Configuración de políticas de grupo (GPO) o administración de dispositivos móviles (MDM) para restringir el acceso a sitios de IA no autorizados mediante listas de sitios permitidos en el navegador corporativo. Se complementa con extensiones de navegador gratuitas que impiden la función de pegado en sitios específicos. Esta opción no genera registros detallados de prompts, pero constituye una primera barrera de control.

Nivel intermedio (inversión moderada): Uso de proxies web con capacidad de inspección de contenido, como soluciones de filtrado web que permiten registrar el tráfico hacia dominios de plataformas de IA y aplicar reglas básicas de prevención de pérdida de datos (DLP). Algunas soluciones de este tipo están disponibles en modelos de suscripción accesibles para Pymes.

Nivel avanzado (inversión estructurada): Implementación de plataformas especializadas de gateway de IA que ofrecen inspección profunda de prompts, redacción automática de datos sensibles, paneles de control con métricas de uso y cumplimiento, integración con sistemas de gestión de identidades, y políticas granulares por usuario, departamento o herramienta. Estas soluciones están orientadas a organizaciones que ya cuentan con un nivel de madurez intermedio o avanzado en su gobernanza de IA.

A.4 Consideraciones para la implementación

La implementación de un gateway de IA debe considerar los siguientes aspectos:

- Privacidad de los empleados: la inspección de prompts implica el monitoreo de la actividad del usuario, por lo que debe comunicarse de forma transparente mediante la política de uso de IA de la organización. En Costa Rica, el monitoreo de comunicaciones laborales debe realizarse conforme a la normativa laboral vigente y con conocimiento del empleado.
- Cifrado de tráfico: la mayoría de las plataformas de IA utilizan conexiones HTTPS. Para que el gateway pueda inspeccionar el contenido, es necesario implementar inspección TLS (TLS inspection), lo cual requiere la instalación de un certificado raíz corporativo en los dispositivos de la organización.
- Rendimiento: la inspección de contenido puede introducir latencia en las solicitudes. La solución seleccionada debe ser evaluada en términos de rendimiento para no afectar la productividad de los usuarios.
- Alcance: el gateway es efectivo únicamente cuando los usuarios acceden a las plataformas de IA desde los dispositivos y la red controlada por la organización. El uso

de dispositivos personales o redes externas puede evadir estos controles, por lo que debe complementarse con políticas organizacionales y sensibilización al personal.

A.5 Relación con el marco de gobernanza propuesto

El gateway de IA no es un sustituto de la gobernanza organizacional, sino un habilitador técnico que refuerza el cumplimiento de las políticas definidas en el marco. Su implementación contribuye directamente a los siguientes componentes:

- Componente 2 – Gestión del riesgo: mitiga los riesgos de exfiltración de datos y uso no autorizado de herramientas de IA.
- Componente 4 – Protección de datos: automatiza la aplicación de las reglas de clasificación de información y previene el ingreso de datos sensibles en plataformas externas.
- Componente 5 – Supervisión y mejora continua: proporciona registros de auditoría que alimentan los indicadores de desempeño definidos en la sección 5.9, particularmente el indicador de incidentes de privacidad y el de cumplimiento de la política de uso.

La incorporación progresiva de controles técnicos como el gateway de IA permite que el marco de gobernanza trascienda el plano documental y se materialice en la infraestructura tecnológica de la organización, fortaleciendo así la postura de seguridad de la Pyme frente al uso de inteligencia artificial.