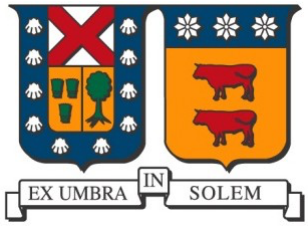
UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



"Desarrollo de un Framework para Gobernanza y Operación de Soluciones de Inteligencia Artificial en una Gerencia de Operaciones de la Industria de Telecomunicaciones"

GONZALO IVAN VALDÉS TORRES

TESINA PARA OPTAR AL GRADO
DE MAGÍSTER EN TECNOLOGÍAS DE
LA INFORMACIÓN

Profesor Guía: PABLO CRUZ

CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☐ Memoria o trabajo de título ☒ Tesis de Postgrado

Título del trabajo: Desarrollo de un Framework para Gobernanza y Operación de Soluciones de Inteligencia Artificial en una Gerencia de Operaciones de la Industria de Telecomunicaciones

Nombre del candidato(a): Gonzalo Iván Valdés Torres

Carrera / Grado: Magíster en Tecnologías de la Información.

Campus: Vitacura **Departamento:** informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, **Pablo Cruz**, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por **(marcar una opción)**:

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

_____

_____

_____

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 28-10-2026 **Firma:** _____

Estudiante o Candidato(a):

Fecha: 28-10-2026 **Firma:** _____

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Desarrollo de un Framework para Gobernanza y Operación de Soluciones de Inteligencia Artificial en una Gerencia de Operaciones de la Industria de Telecomunicaciones

Gonzalo Valdés Torres

Avenida Santa Filomena 12605, Colina, Región Metropolitana

gvaldestorres@gmail.com

Resumen: En el sector de telecomunicaciones, la Gerencia de Operaciones (GOC) enfrenta el desafío de optimizar procesos y avanzar hacia redes autónomas, donde la inteligencia artificial (IA) es un catalizador clave. No obstante, la ausencia de una estructura formal limita su adopción, generando iniciativas desarticuladas, riesgos no gestionados y compras tecnológicas ineficientes. Esta tesina aborda dicha problemática mediante el diseño de un framework de gobernanza y operación para soluciones de IA, fundamentado en los estándares internacionales ISO/IEC 42001, ISO/IEC 23894 e ISO/IEC TR 24028. El modelo se articula en tres niveles: estratégico, de gobernanza y operacional. La información levantada mediante una encuesta a profesionales de la GOC muestra que el marco destaca en fundamentar y elevar la calidad de las decisiones estratégicas, logrando consenso pleno en la priorización justificada de iniciativas y en la asignación explícita de responsabilidades (accountability). Asimismo, los resultados confirman un impacto directo en la eficiencia operativa y en la adquisición de activos tecnológicos, facilitando la evaluación objetiva de plataformas y el escalamiento estandarizado de modelos. La propuesta consolida a la IA como un activo corporativo auditable, seguro y alineado con los objetivos de la Gerencia de Operaciones.

Palabras Clave: framework, gobernanza de IA, ISO/IEC 42001, inteligencia artificial, telecomunicaciones.

1 Introducción

1.1 Contexto, Motivación y problemática

La industria de telecomunicaciones se encuentra en un proceso continuo de transformación digital, impulsado por la necesidad de hacer más eficientes sus operaciones, reducir los tiempos de respuesta y ofrecer servicios cada vez más inteligentes y personalizados. En este escenario competitivo, la Gerencia de Operaciones (GOC) cumple un rol importante al ser responsable de operar y mantener procesos críticos como la gestión de redes, la atención de incidentes y el aseguramiento de la calidad del servicio del core de la red. Para enfrentar estos desafíos, muchas organizaciones han comenzado a incorporar tecnologías emergentes, y entre ellas la inteligencia artificial (IA) destaca como una de las más prometedoras. Su capacidad para automatizar tareas, identificar patrones complejos y respaldar decisiones basadas en datos la convierte en una herramienta estratégica. Según NTT Data, la IA y la automatización están redefiniendo el sector telecomunicaciones al mejorar la eficiencia operativa y generar ingresos sostenibles [1]. Asimismo, estudios recientes destacan que la IA permite optimizar el tráfico de red, reducir costos operativos y mejorar la calidad del servicio mediante capacidades de predicción y adaptación en tiempo real [2].

La motivación de esta tesina surge de la creciente necesidad de estructurar el uso de IA en contextos operativos, donde su implementación suele ser fragmentada, reactiva y poco alineada con los objetivos estratégicos del negocio. En muchas organizaciones, los proyectos de IA se desarrollan como iniciativas aisladas, sin una gobernanza clara ni criterios comunes para su evaluación, escalabilidad o sostenibilidad. Esta situación genera riesgos operativos, dificulta la trazabilidad de decisiones automatizadas y limita el valor que la IA puede aportar a la organización. Diversos expertos advierten que los desafíos de gobernanza de IA incluyen la falta de marcos normativos, riesgos éticos y dificultades para garantizar transparencia y confiabilidad en sectores regulados como las telecomunicaciones [3][4].

La problemática central que aborda esta tesina es la ausencia de un marco normativo y operativo que permita gestionar de forma segura, auditable y alineada con el ciclo de vida de las soluciones de IA en una Gerencia de Operaciones. En particular, se identificó la necesidad de contar con un framework que integre estándares internacionales, como la norma ISO/IEC 42001[5] para sistemas de gestión de IA, que facilita tanto la toma de decisiones informadas como la adquisición estratégica de activos tecnológicos (plataformas, datos y modelos). Esta norma proporciona un enfoque sistemático para gestionar riesgos, asegurar transparencia y demostrar el uso responsable de sistemas de IA en organizaciones que desarrollan o utilizan estas tecnologías [6][7].

1.2 Definición técnica del problema

La creciente incorporación de soluciones de inteligencia artificial (IA) en la industria de telecomunicaciones ha generado un entorno operativo cada vez más complejo, donde la automatización, el análisis predictivo y la toma de decisiones basadas en datos se han vuelto elementos clave para la eficiencia y competitividad. Sin embargo, en el contexto específico de la Gerencia de Operaciones (GOC), la adopción de estas soluciones suele carecer de una estructura formal de gobernanza y operación que permita gestionar de forma segura, trazable y alineada el ciclo de vida de los sistemas de IA.

Desde una perspectiva técnica, el problema se manifiesta en la ausencia de un framework que articule los procesos, roles, políticas y controles necesarios para garantizar que las soluciones de IA sean desarrolladas, desplegadas y monitoreadas conforme a estándares internacionales. Esta carencia se traduce en:

- **Falta de trazabilidad y auditabilidad de los modelos y decisiones automatizadas**, lo que dificulta su validación, supervisión y mejora continua. Como también riesgos operacionales y éticos no gestionados, derivados de la falta de transparencia en el funcionamiento de los modelos o sistemas de IA, sesgos en los datos y ausencia de mecanismos de control.

- **Desalineación con la estrategia organizacional,** al no existir criterios comunes para priorizar, evaluar o escalar iniciativas de IA.

- **Dificultades en la adquisición y gestión de activos tecnológicos** (plataformas, datos, modelos), debido a la falta de lineamientos técnicos y de gobernanza que orienten su selección, integración y reutilización.

Dado lo anterior, la problemática técnica radica en la necesidad de diseñar un framework de gobernanza y operación para IA que, basado en normas como la ISO/IEC 42001[5], ISO/IEC 23894[8] e ISO/IEC TR 24028[9], permita estructurar un ciclo de vida de IA que sea auditable, seguro y alineado con los objetivos de la Gerencia de Operaciones. Este framework debe habilitar y contribuir a la toma de decisiones informadas y confiables, y facilitar la gestión estratégica de los activos tecnológicos involucrados en el desarrollo y operación de soluciones de inteligencia artificial.

1.3 Estrategia o enfoque de solución adoptado

La estrategia adoptada en esta tesina se basa en el diseño de un framework normativo y operativo que permita estructurar la gobernanza y operación de soluciones de inteligencia artificial (IA) en una Gerencia de Operaciones en la industria de las telecomunicaciones. Este enfoque busca abordar los desafíos identificados como falta de trazabilidad, riesgos no gestionados, baja escalabilidad y desalineación estratégica, asertividad en las decisiones asociadas a la adquisición de activos tecnológicos, mediante la integración de estándares internacionales que aseguren un ciclo de vida de IA auditable, seguro y alineado con los objetivos de la organización donde este inmersa la Gerencia de Operaciones.

El framework propuesto se construye sobre tres pilares normativos principales:

- **ISO/IEC 42001**[5]: como eje central, establece los requisitos para implementar un sistema de gestión de IA, incluyendo políticas, roles, procesos y controles que garanticen el uso responsable y trazable de sistemas inteligentes.

- **ISO/IEC 23894**[8]: aporta lineamientos para la gestión de riesgos específicos de IA, permitiendo identificar, evaluar y mitigar amenazas éticas, operativas y técnicas.

- **ISO/IEC TR 24028**[9]: complementa el enfoque con criterios de confiabilidad, robustez y resiliencia de sistemas de IA, fundamentales para entornos críticos como operaciones de telecomunicaciones.

Para validar la efectividad del framework, se adopta una metodología empírica basada en la aplicación de una encuesta estructurada a actores clave del proceso (tomadores de decisiones, arquitectos de soluciones, equipos de desarrollo). Este instrumento permite relevar la percepción sobre el impacto del framework en la calidad de las decisiones y en la eficiencia de la adquisición y gestión de activos tecnológicos.

En síntesis, el enfoque de solución combina rigor normativo, aplicabilidad operativa y validación empírica, con el objetivo de habilitar un entorno de IA gobernado, seguro y generador de valor para la Gerencia de Operaciones.

1.4 Metodología de trabajo para la solución

La metodología adoptada en este trabajo combina un enfoque normativo, basado en estándares internacionales de gestión de inteligencia artificial (IA), con una validación empírica mediante instrumentos de percepción organizacional que para el caso de esta Tesina son encuestas. Esta estrategia busca asegurar que el framework propuesto se analice desde el punto de vista técnico, esté alineado con buenas prácticas globales y sea aplicable al contexto operativo de una Gerencia de Operaciones de la industria de las telecomunicaciones.

1.4.1 Diseño del Framework

La metodología de desarrollo del framework se estructuró en tres fases:

- **Revisión normativa:** Se realizó un análisis detallado de las normas ISO/IEC 42001[5] (Sistema de Gestión de IA), ISO/IEC 23894[8] (Gestión de Riesgos en IA) y ISO/IEC TR 24028[9] (Confiabilidad de Sistemas de IA), con el objetivo de identificar principios, requisitos y buenas prácticas aplicables al ciclo de vida de soluciones de IA en operaciones.
- **Modelado conceptual:** A partir de los lineamientos normativos, se construyó una figura conceptual que organiza el framework en tres capas: estratégica ("el porqué"), normativa ("reglas del juego") y operativa ("el cómo"), integrando componentes como visión, políticas, métricas, infraestructura, seguridad y monitoreo.
- **Definición de componentes operativos:** En esta fase se definieron los procesos, roles, artefactos y controles asociados a cada etapa del ciclo de vida de la IA, desde el diseño hasta el mantenimiento, asegurando trazabilidad, auditabilidad y alineación estratégica.

1.4.2 Hipótesis y Método de validación

La hipótesis central de esta tesina es:

"La implementación de un framework de gobernanza y operación para inteligencia artificial contribuye a la mejora en la calidad de la toma de decisiones al hacerlas más informadas y auditables, facilitando el desarrollo de las soluciones con IA como la adquisición estratégica de activos tecnológicos (plataformas, datos y modelos)"

Donde las variables son las siguientes:

- **Variable Independiente:** Implementación del Framework de gobernanza y operación para soluciones con IA.

- **Variable Dependiente:** Calidad en la toma de decisiones (como efecto de la implementación del framework).

Para evaluar la efectividad del framework y validar la hipótesis de investigación, se implementó una metodología basada en una encuesta estructurada:

- **Diseño de la encuesta:** Se elaboró una encuesta dirigida a actores clave de la GOC (tomadores de decisiones, arquitectos de soluciones, equipos de desarrollo), con preguntas orientadas a medir la percepción sobre:

    - La mejora en la calidad de la toma de decisiones.
    - La trazabilidad y auditabilidad de los procesos de IA.
    - La facilitación en la adquisición y gestión de activos tecnológicos.

La escala que será utilizada es la de Likert (1 = muy en desacuerdo a 5 = muy de acuerdo) con el fin de captar matices en las respuestas que puedan enriquecer y mejorar el análisis posterior.

- **Aplicación de la encuesta:** La encuesta se distribuye de forma digital, garantizando anonimato y voluntariedad. Se busca una muestra representativa de perfiles técnicos y estratégicos dentro de la Gerencia de Operaciones.

- **Análisis de resultados:** Se aplican técnicas de análisis descriptivo y correlacional para identificar patrones de percepción, validar la hipótesis y detectar oportunidades de mejora en el framework.

Con base en los resultados obtenidos, se propone una iteración del framework que incorpore retroalimentación de los participantes, fortaleciendo su aplicabilidad y alineación con las necesidades reales de la Gerencia de Operaciones

1.5 Estructura del Informe

En el segundo capítulo se revisa el marco teórico y estado del arte de los conceptos claves que se utilizarán dentro de este trabajo. En el tercer capítulo, se aborda el desarrollo del framework, en la cuarto capitulo mediante la ejecución de la encuesta se valida el real impacto del marco de trabajo siguiendo los pasos de la metodología propuesta en el punto 1.4. Finalmente, se presentan las conclusiones de esta tesina.

2 Marco teórico y Estado del arte

El desarrollo de soluciones de inteligencia artificial (IA) en sectores críticos como telecomunicaciones requiere un sustento teórico que combine aspectos tecnológicos, normativos y organizacionales. Diversos estudios destacan que la IA no solo constituye una herramienta de automatización, sino también un habilitador estratégico para la transformación digital, capaz de optimizar procesos, anticipar fallas y mejorar la calidad del servicio en tiempo real [10]. En particular, la literatura reciente enfatiza que la integración de IA en operaciones de red permite reducir costos, incrementar la eficiencia y garantizar servicios más confiables y personalizados [12].

Como parte del marco teórico se presentan los siguientes conceptos claves:

2.1 Framework

Un *framework* se entiende como una estructura conceptual y normativa que organiza principios, procesos y herramientas para abordar un problema de manera sistemática. Según ISO/IEC/IEEE 42010[5], los frameworks permiten estandarizar la descripción de arquitecturas, facilitando la comunicación y revisión de soluciones tecnológicas [13]. En el mismo sentido, IEEE 2413-2019[11] lo define como un marco arquitectónico que integra preocupaciones comunes en sistemas complejos, asegurando interoperabilidad y consistencia [14].

2.2 Inteligencia Artificial

La inteligencia artificial (IA) se entiende como la capacidad de sistemas computacionales para ejecutar tareas que requieren inteligencia humana, tales como razonamiento, aprendizaje y comprensión del lenguaje. La IA corresponde a sistemas capaces de analizar datos, reconocer patrones y tomar decisiones con rapidez y precisión [16]. En el mismo sentido, la norma ISO/IEC 22989:2022[17] la define como un campo de la informática orientado al desarrollo de sistemas que perciben su entorno y actúan de manera autónoma para alcanzar objetivos [18]. Complementariamente, el IEEE enfatiza que la IA constituye una disciplina que busca emular funciones cognitivas humanas, incluyendo el aprendizaje y la toma de decisiones [19].

2.3 Gobernanza de IA

La gobernanza de la inteligencia artificial (IA) se entiende como el conjunto de políticas, procesos, roles y estándares que aseguran que el desarrollo y uso de sistemas de IA se realice de manera ética, transparente, segura y alineada con los objetivos organizacionales.

Documentos de política internacional destacan que la gobernanza de IA es esencial para garantizar interoperabilidad, confianza y cumplimiento regulatorio en sectores críticos como telecomunicaciones, donde las decisiones automatizadas tienen impacto directo en la calidad del servicio y en la seguridad de los usuarios [20].

2.4 ISO 42001

La ISO/IEC 42001:2023[5] es el primer estándar internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Inteligencia Artificial (SGIA) dentro de una organización. Su objetivo es asegurar que el desarrollo y uso de sistemas de IA se realice de manera ética, transparente, segura y alineada con los objetivos estratégicos del negocio [20].

De acuerdo con la International Organization for Standardization (ISO), esta norma proporciona un marco sistemático que incluye políticas, roles, métricas y procesos para gestionar el ciclo de vida de la IA, desde el diseño hasta el monitoreo [20]. Deloitte enfatiza que ISO/IEC 42001[5] permite a las organizaciones demostrar responsabilidad, gestionar riesgos y cumplir con regulaciones, especialmente en sectores críticos como telecomunicaciones [21].

Asimismo, expertos como Brisett señalan que la norma habilita una gobernanza clara de la IA, abordando desafíos como la falta de transparencia, la trazabilidad de decisiones automatizadas y la necesidad de confianza en sistemas inteligentes [22].

2.5 Estado del Arte

La integración de inteligencia artificial (IA) en la industria de las telecomunicaciones ha generado un impacto significativo en la eficiencia operativa, la confiabilidad de las redes y la experiencia del cliente. A continuación, se presentan casos relevantes de implementación en empresas líderes del sector, junto con iniciativas colaborativas que buscan estandarizar y acelerar la adopción de redes autónomas a través de IA.

2.5.1 Verizon: Optimización de red y mantenimiento predictivo

Verizon ha incorporado algoritmos de IA para detectar y prevenir interrupciones de red antes de que afecten a los usuarios, fortaleciendo su reputación de confiabilidad. La complejidad de gestionar una operación global exigía soluciones más eficientes.

Soluciones aplicadas: análisis de datos en tiempo real para detección temprana de fallos, optimización automatizada de la red y estrategias de mantenimiento predictivo.

Resultados: reducción significativa de interrupciones, mejora en tiempos de respuesta y aumento de la satisfacción del cliente [23].

2.5.2 Deutsche Telekom: Eficiencia Operativa y Gestión Energética

La empresa alemana enfrentó el reto de reducir costos operativos y consumo energético sin comprometer la calidad del servicio.

Soluciones aplicadas: automatización de operaciones de red mediante IA, gestión energética inteligente y personalización de servicios al cliente.

Resultados: disminución de costos, ahorro energético y mejora en la experiencia del cliente [24].

2.5.3 TM Forum y las redes autónomas

TM Forum, asociación global de telecomunicaciones y tecnología, impulsa la transición hacia redes altamente autónomas (nivel 4) mediante su Autonomous Networks Toolkit.

Componentes principales: arquitectura estandarizada, niveles de madurez (0–5), guías de implementación, APIs abiertas y casos de uso como redes privadas 5G.

Beneficios reportados: reducción de costos operativos hasta un 55%, mejora de satisfacción del cliente hasta un 71% y ahorro energético de hasta un 21% [25].

Ejemplos de adopción: Telefónica, que avanza hacia redes hiperautomatizadas en su estrategia 2025 [26], y China Mobile, que desplegó la red privada 5G más grande del mundo aplicando principios de autonomía [27].

Los casos revisados muestran que la IA en telecomunicaciones no solo optimiza procesos técnicos, sino que también reduce costos, mejora la sostenibilidad y fortalece la relación con los clientes. Además, iniciativas como las de TM Forum evidencian la importancia de contar con marcos de referencia estandarizados para guiar la transición hacia redes autónomas de próxima generación a través del uso de IA.

3 Desarrollo de la solución

3.1 Arquitectura conceptual Framework

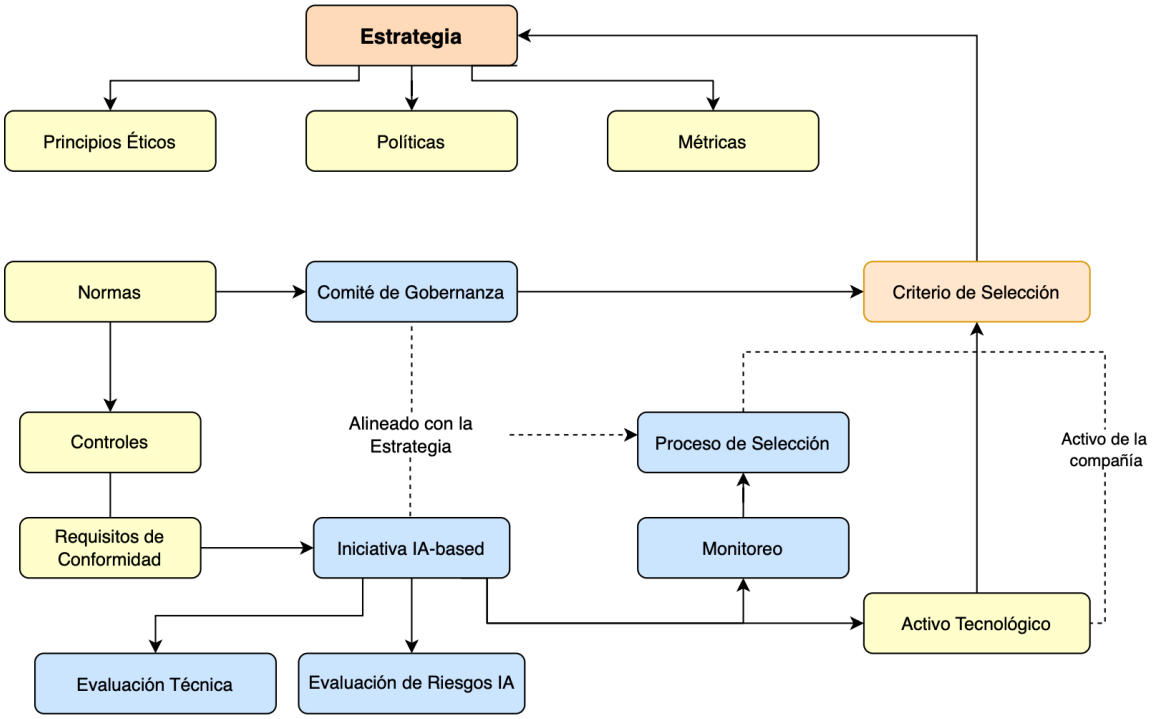


Figura 1. Arquitectura conceptual del *framework* de gobernanza y operación de IA

El diagrama conceptual presentado en la **Figura 1** constituye un instrumento preliminar que organiza y relaciona los conceptos fundamentales involucrados en la adopción de iniciativas de inteligencia artificial (IA). Su propósito es ofrecer una visión estructurada que permita comprender cómo las decisiones estratégicas se traducen en mecanismos de gobernanza y prácticas operacionales, preparando el terreno para la propuesta del framework basado en la norma ISO/IEC 42001[5].

Cada concepto busca la necesidad de garantizar coherencia, trazabilidad y responsabilidad en el ciclo de vida de las soluciones IA. A continuación, se explican los elementos del diagrama y su función como preámbulo al diseño del framework.

3.1.1 Nivel estratégico

Estrategia de IA: Define la orientación general y los objetivos organizacionales que justifican el uso de IA. Es el punto de partida que condiciona el resto de los elementos.

Principios éticos: Incorporan valores como transparencia, equidad y explicabilidad, asegurando que las iniciativas respondan a criterios de responsabilidad social y organizacional.

Políticas: Formalizan lineamientos internos que regulan el diseño, uso y monitoreo de soluciones IA, estableciendo límites y expectativas claras.

Métricas: Proveen indicadores de desempeño e impacto, habilitando la evaluación de resultados y la retroalimentación hacia la estrategia.

3.1.2 Nivel de gobernanza

Normas: Integran estándares internacionales que aportan rigor técnico y criterios de confiabilidad, seguridad y gestión de riesgos.

Comité de gobernanza IA: Órgano responsable de supervisar y coordinar la selección de iniciativas, garantizando alineación con la estrategia y cumplimiento normativo. La gobernanza requiere una estructura humana y cuantitativa. El Comité asegura la asignación de responsabilidades y la rendición de cuentas.

Roles y responsabilidades: Definen funciones claras para los actores involucrados, promoviendo una cultura de responsabilidad compartida.

Criterios de selección: Establecen reglas y ponderaciones que permiten priorizar iniciativas en función de su valor estratégico, ético y técnico. Por ejemplo, el criterio de selección puede priorizar iniciativas IA orientadas a la optimización de redes, en línea con la estrategia de eficiencia operacional de la Gerencia.

3.1.3 Nivel operacional

Controles: Implementan medidas concretas para asegurar el cumplimiento de políticas y normas.

Requisitos de conformidad: Consolidación de obligaciones técnicas, regulatorias y éticas que se verifican en la evaluación de cada iniciativa.

Evaluación técnica: Verifica la factibilidad tecnológica, calidad de datos y robustez de los modelos.

Evaluación de riesgos IA: Identifica y mitiga riesgos específicos asociados al uso de IA, en línea con ISO/IEC 23894[8]. Esto asegura que la Iniciativa IA-based sea evaluada no solo por su capacidad técnica, sino también por su robustez y confiabilidad.

Proceso de selección: Integra los resultados de las evaluaciones y determina la viabilidad de la iniciativa.

Monitoreo: Observa el desempeño y los riesgos durante la operación, habilitando ciclos de mejora continua.

Activo organizacional: Representa la transformación de la iniciativa IA en un activo tecnológico que modifica procesos y capacidades de la organización.

Esta disposición jerárquica y funcional garantiza que cualquier solución tecnológica considerada como IA-Based no sea un elemento independiente, sino un activo gobernado que responde a un marco de control auditable, interoperable y alineado con los estándares internacionales.

3.1.4 Relación conceptos con requisitos normativos ISO/IEC

Cada concepto que forma parte de la arquitectura conceptual del framework tiene relación con los estándares internacionales ISO/IEC 42001[5], ISO/IEC 23894[8] y TR 24028[9]. De esta manera, se evidencia que el framework diseñado no surge de manera aislada, sino como la formalización auditable de un modelo conceptual previamente estructurado.

3.2 Descripción del Framework

En este apartado se describe el Framework para Gobernanza y Operación de soluciones con IA. Este marco de trabajo integra lineamientos técnicos y de gobernanza para asegurar que las soluciones sean desarrolladas, desplegadas y monitoreadas de forma coherente, auditable y alineada con los objetivos estratégicos de la organización. Como también contribuir en la mejora de la toma de decisiones como, por ejemplo, compra de activos.

Para desarrollar el framework se toma un enfoque normativo basado en estándares internacionales de gestión de inteligencia artificial (IA). Esta estrategia busca garantizar que el framework propuesto sea técnicamente robusto, alineado con buenas prácticas globales y aplicable al contexto operativo de una Gerencia de Operaciones en telecomunicaciones.

El desarrollo del framework se estructuró en tres fases:

- Revisión normativa: Se realizo un análisis de las normas ISO/IEC 42001[5] (Sistema de Gestión de IA), ISO/IEC 23894[8] (Gestión de Riesgos en IA) y ISO/IEC TR 24028[9] (Confiabilidad de Sistemas de IA), con el objetivo de identificar principios, requisitos y buenas prácticas aplicables al ciclo de vida de soluciones de IA en operaciones.

- Modelado conceptual: A partir de los lineamientos normativos, se construyó una figura conceptual que organiza el framework en tres capas: estratégica (“el por qué”), normativa (“reglas del juego”) y operativa (“el cómo”), integrando componentes como visión, políticas, métricas, infraestructura, seguridad y monitoreo.

- Definición de componentes operativos: Se detallan los procesos, roles, artefactos y controles asociados a cada etapa del ciclo de vida de la IA, desde el diseño hasta el mantenimiento, asegurando trazabilidad, auditabilidad y alineación estratégica.

La decisión de fundamentar el desarrollo del framework en normas ISO se basa en contar con una base técnica confiable, reconocida internacionalmente y adaptable al contexto operativo de una Gerencia de Operaciones en telecomunicaciones. Las normas ISO/IEC relacionadas con inteligencia artificial, en particular la ISO/IEC 42001[5], ISO/IEC 23894[8] y ISO/IEC TR 24028[9], ofrecen lineamientos claros para estructurar procesos, gestionar riesgos y asegurar la confiabilidad de los sistemas inteligentes.

Este enfoque normativo permite:

- Alinear las soluciones de IA con los objetivos estratégicos del negocio, asegurando que su desarrollo y operación respondan a criterios de valor, trazabilidad y sostenibilidad.
- Establecer una gobernanza clara, con roles definidos, métricas de desempeño y políticas organizacionales que regulen el uso responsable de la IA.
- Gestionar riesgos éticos, operacionales y técnicos, mediante prácticas auditables que promuevan la transparencia y la rendición de cuentas.
- Habilitar un ciclo de vida completo y seguro para la IA, desde el diseño hasta el monitoreo, facilitando la mejora continua y la escalabilidad de las soluciones.

Además, al adoptar estándares internacionales, el framework se vuelve interoperable y adaptable a distintos entornos regulatorios, lo que facilita su implementación en organizaciones que operan bajo exigencias normativas estrictas. En este sentido, el uso de normas ISO no solo aporta rigor técnico, sino que también habilita una evolución progresiva hacia entornos más inteligentes, resilientes y autónomos, donde la IA no solo apoya decisiones, sino que participa activamente en la gestión de la red.

3.3 Diseño del Framework

El diseño del framework para la gobernanza y operación de sistemas de Inteligencia Artificial (IA) se fundamenta en la necesidad de garantizar un desarrollo responsable, seguro y alineado con los objetivos estratégicos de la organización. Para ello, se adopta como referencia la norma ISO/IEC 42001:2023[5], que establece los requisitos para un sistema de gestión de IA, y la guía ISO/IEC TR 24028:2020[9], que proporciona criterios sobre seguridad y confiabilidad de los sistemas de IA. La integración de ambos marcos permite articular un enfoque que abarca la estrategia, la gobernanza y la operación.

3.3.1 El “Porqué”: Estrategia

La dimensión estratégica responde a la justificación y propósito del uso de IA en la organización, para el caso de esta Tesina es la Gerencia de Operaciones de una empresa de telecomunicaciones, en concordancia con los principios de la ISO/IEC 42001[5]:

- Visión: Definir una visión organizacional sobre el rol de la IA, alineada con los objetivos de negocio y los valores institucionales. Según ISO/IEC 42001[5], la visión debe integrarse en la política de IA y reflejar el compromiso de la alta dirección.
- Gestión de Riesgos: Adoptar un enfoque sistemático para identificar, evaluar y mitigar riesgos asociados al uso de IA. La norma exige procesos de gestión de riesgos que incluyan aspectos técnicos, regulatorios y éticos.
- Responsabilidad y Ética: Incorporar principios éticos como transparencia, explicabilidad y equidad. TR 24028[9] enfatiza la necesidad de evaluar la confiabilidad de los sistemas, incluyendo sesgos y vulnerabilidades que puedan afectar la responsabilidad organizacional.

3.3.2 Reglas del Juego: Gobernanza

La gobernanza establece las condiciones habilitantes para un uso responsable de la IA, en línea con los requisitos de gestión de ISO/IEC 42001[5]:

- Política de IA: La norma requiere que las organizaciones definan una política formal de IA, que regule el diseño, uso y monitoreo de soluciones, incluyendo criterios de validación y límites de autonomía.
- Métricas: ISO/IEC 42001[5] establece la necesidad de indicadores de desempeño para evaluar la eficacia del sistema de gestión de IA. Estos KPIs deben incluir seguridad, confiabilidad y alineación con objetivos estratégicos.
- Roles y Responsabilidades: La norma exige asignar funciones claras a los actores involucrados (desarrolladores, usuarios, auditores, líderes), promoviendo una cultura de responsabilidad compartida. TR 24028[9] complementa este aspecto al recomendar la definición de responsabilidades en la gestión de riesgos de seguridad.

3.3.3 El "Cómo": Ciclo de Vida y Operación

La dimensión operacional traduce la estrategia y gobernanza en prácticas concretas, vinculadas con los requisitos de gestión de ISO/IEC 42001[5] y los lineamientos de seguridad de TR 24028[9].

Ciclo de Vida de la Solución

- Diseño de Casos de Uso: Identificación de problemas relevantes y definición de objetivos, conforme a la política de IA.
- Elección de Algoritmos: Selección basada en criterios técnicos, éticos y de negocio. TR 24028[9] recomienda evaluar la robustez y confiabilidad de los algoritmos.
- Despliegue de Modelos: Validación funcional e integración en plataformas operativas, cumpliendo con los requisitos de control establecidos en ISO/IEC 42001[5].
- Monitoreo y Mantenimiento: Supervisión continua del desempeño, detección de desviaciones y actualización de modelos. La norma exige procesos de mejora continua y TR 24028[9] enfatiza la necesidad de pruebas de resiliencia.

Componentes Operacionales

- Infraestructura: Recursos tecnológicos (hardware, software, redes) que deben cumplir con requisitos de seguridad y disponibilidad.
- Fuente de Datos: Identificación de fuentes confiables y representativas, conforme a los principios de calidad de datos de ISO/IEC 42001[5].
- Recopilación de Datos: Procesos de adquisición, limpieza y etiquetado, garantizando trazabilidad y cumplimiento normativo.
- Seguridad: Protección de datos y ciberseguridad, en línea con TR 24028[9], que establece criterios para evaluar vulnerabilidades y resiliencia.

- Plataformas en Operación: Integración con sistemas existentes, asegurando interoperabilidad y escalabilidad, como exige ISO/IEC 42001[5].

Se presenta en la **Figura 2** el Framework para la Gobernanza y Operación de soluciones con Inteligencia artificial para la Gerencia de Operaciones de la industria de la Telecomunicaciones en el siguiente diagrama:

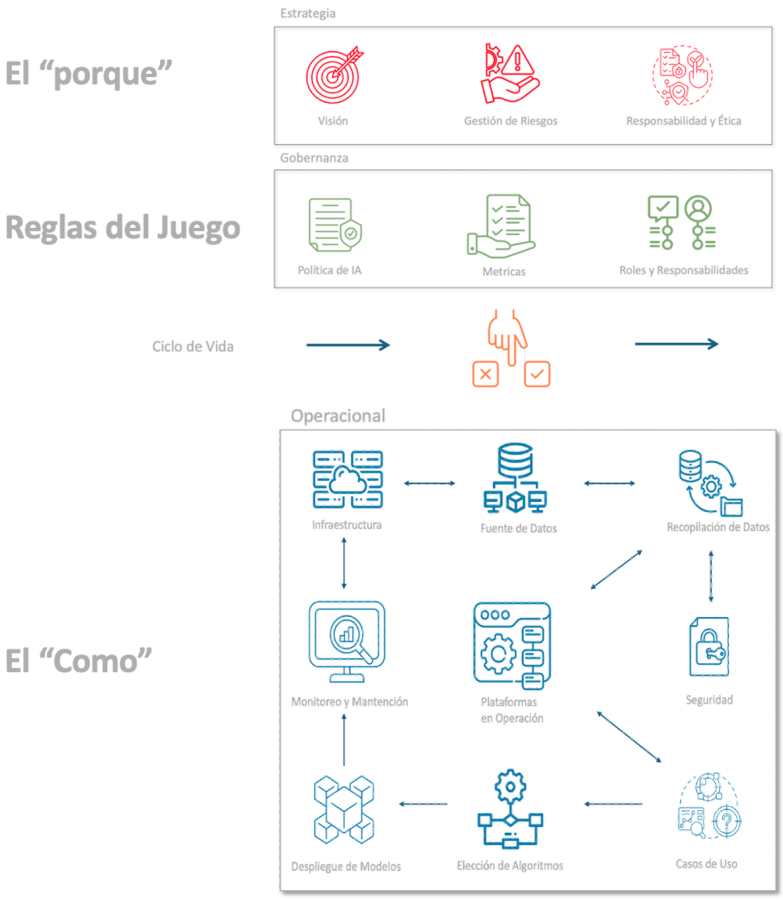


Figura 2. *Framework* para la Gobernanza y Operación de soluciones con IA

El desarrollo de la solución expuesto en este capítulo muestra una progresión desde la arquitectura conceptual, que organiza los elementos estratégicos, de gobernanza y operacionales, hasta la tabla de correspondencia normativa, que evidencia la trazabilidad de cada concepto frente a los estándares internacionales ISO/IEC 42001[5], ISO/IEC 23894[8] y TR 24028[9]. Posteriormente, la descripción del framework establece sus fundamentos normativos y su aplicabilidad en el contexto de operaciones de telecomunicaciones, mientras que el diseño del framework traduce dichos fundamentos en componentes concretos, roles definidos y prácticas auditables. De esta manera, el capítulo demuestra que la solución propuesta no surge de manera aislada, sino como la formalización de un modelo conceptual previamente estructurado, garantizando coherencia, responsabilidad y alineación estratégica.

3.4 Propuesta de Implementación del Framework

Esta sección tiene como propósito proponer como poner en operación el modelo teórico propuesto, mostrando cómo cada componente se traduce en prácticas concretas dentro de la Gerencia. Para ello, se expone el "modo de uso" de cada elemento, especificando los factores que activan cada proceso, los roles responsables de su ejecución, los pasos a seguir y los resultados esperados que permiten evidenciar el cumplimiento tanto normativo como estratégico.

El desarrollo se presenta organizado por los elementos del framework, proporcionando para cada uno una definición funcional que abarca desde el criterio de aplicación hasta la generación de evidencia, facilitando así su adopción para cada una de las capas (Estrategia, Gobernanza y Operacional). Cada elemento del framework según la capa a cual pertenece se describirá utilizando la siguiente estructura:

- **Objetivo:** Para qué sirve.
- **Criterio de Aplicación:** Cuándo se usa este elemento.
- **Roles Responsables:** Quién lo hace.
- **Procedimiento:** Qué pasos seguir.
- **Entregable estandarizado:** Entregables del elemento.

3.4.1 Estrategia

La estrategia se inicia definiendo la visión (ver **Tabla 1**) que en su esencia traduce metas de negocio en objetivos concretos y medibles de IA. Liderado por el CTO, la Gerencia de Operaciones y el Comité de Estrategia de IA, sigue las fases de definir, accionar, validar, documentar y formalizar acuerdos. Su propósito central radica en alinear estrictamente las capacidades técnicas con los lineamientos corporativos. El siguiente paso es establecer los límites de seguridad y riesgos aceptables. La visión marca el rumbo, pero la gestión de riesgos asegura que ese camino se recorra dentro de parámetros seguros y responsables.

Con los riesgos identificados y clasificados según lo detallado en **Tabla 2**, resulta imprescindible asignar responsabilidades claras y traducir los principios éticos en controles técnicos verificables tal como se presenta en la **Tabla 4**. De este modo, la gestión de riesgos no queda como un ejercicio abstracto, sino que se conecta directamente con la responsabilidad humana y la ética aplicada en cada decisión de IA.

Tabla 1. Ficha de implementación operacional del elemento visión

Elemento	**Visión**
Objetivo	Traducir las metas abstractas de negocio, Gerencia en objetivos de Inteligencia Artificial medibles y concretos.
Criterio de Aplicación	Planificación Estrategica o al inciar el area de IA
Roles Responsables	CTO, Gerente de Operaciones y Comité de Estrategia de IA
Procedimiento	1. **Definir:** La Alta Dirección declara una meta por ejemplo de Optimizar la red en un 30%. 2. **Acción:** El líder de IA debe convertir esa meta en un objetivo técnico de la solución de IA (ej. "Implementar modelos predictivos de mantenimiento con un accuracy >90% para Q3"). 3. **Validar:** Revisar cumplimiento estratégico. 4. **Documentar:** Definir recursos, plazos y responsables para lograr ese objetivo, asegurando que la tecnología sirva a la estrategia 5. **Aprobar:** Formalizar la decisión por parte de los responsables de este elemento
Entregable estandarizado	Documento formal aprobado con el Plan Estrategico y/o inicio de area IA

Tabla 2. Ficha de implementación operacional del elemento Gestión de Riesgos

Elemento	**Gestión de Riesgos**
Objetivo	Establecer límites de seguridad y definir qué riesgos son aceptables antes de aprobar o desarrollar proyectos de IA.
Criterio de Aplicación	Se utiliza antes de aprobar cualquier proyecto de IA o frente a cambios regulatorios relevantes.
Roles Responsables	Oficial de Cumplimiento, Gestor de Riesgos, Líderes de Proyecto.
Procedimiento	1. **Definir umbral de riesgo:** Establecer institucionalmente los límites aceptables (ej. "No se aceptan soluciones caja negra en diagnósticos críticos"). 2. **Acción:** Analizar riesgos propios de la IA (sesgo algorítmico, alucinación del modelo, vulnerabilidades técnicas). 3. **Evaluar Riesgos:** Clasificar cada riesgo según probabilidad e impacto, dentro de los límites estratégicos definidos. 4. **Tratar Riesgos:** Decidir si el riesgo se mitiga, se acepta, se transfiere o se evita. 5. **Documentar resultados:** Registrar decisiones y responsables en la matriz de riesgos.
Entregable estandarizado	Matriz de Riesgos de IA aprobada por la Gerencia, con clasificación, responsables y plan de tratamiento documentado.

Tabla 3. Ficha de implementación operacional del elemento Responsabilidad y Ética

Elemento	**Responsabilidad y Ética**
Objetivo	Garantizar que exista una persona responsable (accountable) por las decisiones de la IA y que los principios éticos se traduzcan en controles técnicos verificables.
Criterio de Aplicación	Se aplica al conformar el Comité de Gobernanza de IA o al iniciar un nuevo proyecto que requiera supervisión ética.
Roles Responsables	Comité de Gobernanza de IA, Recursos Humanos, Líderes de Ética de Datos.
Procedimiento	1. **Asignar roles formales:** Definir quién tiene autoridad para aprobar, detener o modificar un modelo. Elaborar una matriz RACI (Responsible, Accountable, Consulted, Informed). 2. **Seleccionar controles éticos:** Traducir cada principio en una acción técnica concreta. Ejemplo: Si el principio es "Transparencia", el control aplicado será "Implementar tarjetas de modelo (Model Cards) para explicar el funcionamiento". Ejemplo: Si el principio es "Justicia", el control será "Ejecutar pruebas de paridad estadística en el dataset". 4. **Definir supervisión humana:** Establecer puntos críticos del ciclo de vida donde un humano debe validar la salida de la IA (human-in-the-loop). 5. **Documentar decisiones:** Registrar controles aplicados, responsables y resultados en un documento formal.
Entregable estandarizado	Matriz RACI aprobada por el Comité de Gobernanza y Declaración de Aplicabilidad (SoA) de controles éticos, firmada por responsables designados.

3.4.2 Gobernanza

Una vez redactada y formalizada la política de IA según la ficha de implementación de la **Tabla 4**, corresponde ponerla en operación mediante métricas que permitan evaluar si las reglas del juego se cumplen en la práctica. La política establece el marco normativo, mientras que las métricas ofrecen la evidencia cuantitativa de su cumplimiento.

Las métricas implementadas según la **Tabla 5**, por sí solas, no garantizan gobernanza si no existe claridad sobre quién debe actuar frente a los resultados. Por ello, la definición de roles y responsabilidades tal como se muestra en **Tabla 6** asegura que cada indicador tenga un responsable directo, eliminando ambigüedades y fortaleciendo la rendición de cuentas.

Tabla 4. Ficha de implementación operacional del elemento Política de IA

Elemento	Politica de IA
Objetivo	Establecer las "reglas del juego" oficiales. No solo dice qué se quiere hacer (la política), sino cómo se debe operar técnicamente para cumplirlo (estándares y procedimientos).
Criterio de Aplicación	Se activa al fundar el gobierno de IA y se actualiza anualmente, o cuando se integra una nueva tecnología disruptiva (ej. adoptar GenAI).
Roles Responsables	Comité de Gobernanza de IA, CISO (Seguridad) y Líderes Técnicos.
Procedimiento	1. **Redacción de Politica:** La alta dirección firma la política general (ej. "Toda IA debe ser explicable"). 2. **Acción :** Los líderes técnicos traducen esa política en un procedimiento estándar (SOP). Ejemplo: Se prohibe el uso de algoritmos "caja negra" en sistemas criticos de dignóstico de red. 3. **Selección de Controles:** Definir qué controles específicos se aplicarán obligatoriamente en los proyectos o iniciativas. Ejemplo: Cada modelo desplegado debe incluir un informe de interpretabilidad, donde se detallen las variables mas influyentes en la predicción de fallas. 5. **Validación Operativa:** El comité de Gobernanza de IA y el area de Operaciones deben revisar periodicamente que las decisiones técnicas estén alineadas con las politicas definidas.
Entregable estandarizado	Manual de Politicas de IA y Guias de procedimientos técnicos (SOPs).

Tabla 5. Ficha de implementación operacional del elemento Métricas

Elemento	Métricas
Objetivo	Validar con datos si el sistema de IA funciona bien, es seguro y aporta valor. Si no se mide, no se gobierna.
Criterio de Aplicación	Para el monitoreo técnico de modelos en producción el cual debe ser continuo. Para auditorias internas y revisiones de gestión trimestral y/o semestral.
Roles Responsables	Auditor interno, cientifico de datos (para métricas técnicas)
Procedimiento	1. **Definición de KPIs:** Establecer que se medirá. 2. **Acción :** Implementación de KPIs Técnicos (Precición, Latencia, desviación de datos) y de Negocio (ROI, Tasa de adopción, Incidentes éticos reportados) 3. **Auditoria Interna:** Realizar revisiones independientes para asegurar que los equipos están siguiendo los procedimientos definidos en el punto 1. 5. **Monitoreo:** Implementar dashboards automáticos que alerten si un modelo baja su rendimiento.
Entregable estandarizado	Informe de evaluación de desempeño y Reportes de Auditoria de IA.

Tabla 6. Ficha de implementación operacional del elemento Roles y Responsabilidades

Elemento	Roles y Responsabilidades
Objetivo	Eliminar la ambigüedad. Asegurar que cada riesgo y cada tarea de IA tenga un "dueño" con nombre y apellido que rinda cuentas.
Criterio de Aplicación	Al inicio de cualquier proyecto de IA
Roles Responsables	Responsable de Recursos Humanos o asignado para ese rol y rol directivo (Ej: Gerente).
Procedimiento	1. **Mapeo de Competencias:** Identificar qué perfiles son necesarios (ej. "Ingeniero en prompt", "Experto en seguridad", "Cientista de datos"). 2. **Acción :** Asignación formal de roles en donde se designa a las personas y se les comunica sus roles o autoridades por escrito (Ej: El cientista de Datos tiene la autoridad para detener un entrenamiento si es que los datos estan sucios). 3. **Comunicación:** Socializar el organigrama de IA a toda la Gerencia para que todos sepan a quién acudir. 5. **Aprobar:** El comité de Gobernanza debe aprobar la estructura de Roles y Responsabilidades.
Entregable estandarizado	Organigrama de Gobernanza de IA, Descripciones de Cargo Actualizadas y Matriz RACI operativa.

3.4.3 Operacional

Las plataformas en operación constituyen el núcleo de esta capa operacional, las que se establecen según la **Tabla 7**, en ellas se anidan los problemas concretos que la Gerencia busca resolver. Estos desafíos se formalizan mediante casos de uso específicos, los cuales se traducen en soluciones basadas en inteligencia artificial que responden directamente a las necesidades de la red.

Una vez delimitado el caso de uso tal como y definido el problema operacional que la IA debe resolver, tal como se indica en la **Tabla 8**, el paso siguiente es proveer la infraestructura adecuada. El caso de uso define el "qué" y la infraestructura habilita el "cómo", asegurando que los recursos tecnológicos estén disponibles para ejecutar la solución.

Con la infraestructura lista según **Tabla 9**, se procede a identificar las fuentes de datos como se detalla en la **Tabla 10** y recopilar la información necesaria. La infraestructura es el entorno, mientras que los datos son el insumo crítico que alimenta los modelos.

Una vez recopilados y preparados los datos como se detalla en **Tabla 11**, la seguridad se convierte en un eje transversal que protege tanto la información como los modelos. La recopilación asegura calidad y trazabilidad, mientras que la seguridad garantiza confidencialidad, integridad y disponibilidad.

Con datos seguros y confiables tomando lo que se detalla en la **Tabla 12**, se habilita la selección de algoritmos o modelos adecuados. La seguridad asegura que el insumo es válido, y la elección de algoritmos traduce ese insumo en soluciones técnicas robustas.

Una vez seleccionado el modelo "campeón" con los pasos indicados en la **Tabla 13**, se procede a su despliegue en entornos productivos. La elección de algoritmos responde al diseño, mientras que el despliegue materializa la solución en la operación real.

Finalmente, el despliegue detallado en la **Tabla 14** no marca el fin del ciclo, sino el inicio de la supervisión continua. El monitoreo y la mantención tal como se detalla en la **Tabla 15** aseguran que el modelo conserve su rendimiento en el tiempo, habilitando ciclos de mejora y reentrenamiento cuando sea necesario.

Tabla 7. Ficha de implementación operacional del elemento Plataformas en Operación

Elemento	**Plataformas en Operación**
Objetivo	Identificar la(s) Plataforma(s) donde se aplicara la solución IA según el caso de uso seleccionado
Criterio de Aplicación	KPI o Metricas que representen alguna degradación de alto impacto para la Gerencia o Negocio
Roles Responsables	Responsable de la Plataforma en Operación
Procedimiento	1. **Disponibilizar:** Disponer la plataforma para aplicación de caso de uso. 2. **Medir:** A traves de KPIs monitorear uso, perfomance, comportamiento de la Plataforma en Operación. 3. **Validar:** Revisar si se cumplen las mejoras en Plataforma en Operación según los criterios de aceptación del Caso de Uso. 4. **Aprobar:** Respnsable de Plataforma en Operación aprueba resultados.
Entregable estandarizado	Informe de metricas y status Plataforma en Operación

Tabla 8. Ficha de implementación operacional del elemento Casos de Uso

Elemento	**Casos de Uso**
Objetivo	Delimitar el alcance funcional y técnico de la solución para resolver un problema operacional específico.
Criterio de Aplicación	Se activa cuando el Comité de Estrategia aprueba una iniciativa o "idea" de IA.
Roles Responsables	Responsable de la plataforma en operación y Arquitecto de Soluciones.
Procedimiento	1. **Levantamiento:** Entrevistar al responsable de la plataforma en operación para identificar y entender el "dolor" o necesidad. 2. **Acción :** Traducir la necesidad en una solución de IA 3. **Criterios de Éxito:** Definir qué métrica determina si el caso de uso está "resuelto" (Ej: Reducir la tasa de falla en acceso de un 20% a un 5%). 4. **Aprobar:** El responsable de la plataforma debe aprobar el caso de uso
Entregable estandarizado	Documento de Definición del Caso de Uso.

Tabla 9. Ficha de implementación operacional del elemento Infraestructura

Elemento	Infraestructura
Objetivo	Proveer los recursos de cómputo y almacenamiento necesarios para entrenar y ejecutar los modelos sin interrupciones.
Criterio de Aplicación	Antes de iniciar el procesamiento de datos o el entrenamiento
Roles Responsables	Ingeniero de DevOps/MLOps y encargado de Infraestructura
Procedimiento	1. **Dimensionamiento:** Estimar la necesidad de GPU/TPU y memoria RAM según la complejidad del modelo esperado. 2. **Acción :** Desplegar los recursos (ej. Clúster de Kubernetes, Instancias EC2/GCP) o configurar servidores locales. 3. **Configuración de entorno:** Instalar librerías base (Ej: PyTorch, TensorFlow, Docker, N8N). 4. **Aprobar:** El responsable Infraestructura aprueba el uso de infraestructura requerido
Entregable estandarizado	Entorno de Desarrollo/Producción Operativo.

Tabla 10. Ficha de implementación operacional del elemento Fuente de Datos

Elemento	Fuente de Datos
Objetivo	Localizar y catalogar los datos brutos que alimentarán al modelo.
Criterio de Aplicación	Inmediatamente después de definir el Caso de Uso.
Roles Responsables	Ingeniero de Datos o dueño de los datos
Procedimiento	1. **Mapeo:** Identificar dónde viven los datos (Bases de datos SQL, Data Lake, APIs externas, logs).. 2. **Acción :** Evaluar la calidad inicial de los datos, verificando si la fuente es confiable, si tiene historico suficiente y si esta actualizada. 3. **Permisos:** Solicitar accesos de lectura a los dueños de los datos. 4. **Aprobar:** El dueño de los datos aprueba el uso de estos.
Entregable estandarizado	Catálogo de Fuentes de Datos y Credenciales de Acceso.

Tabla 11. Ficha de implementación operacional del elemento Recopilación de datos

Elemento	Recopilación de Datos
Objetivo	Mover los datos desde la fuente hasta el entorno de entrenamiento, limpiándolos en el proceso.
Criterio de Aplicación	Durante la fase de preparación de datos.
Roles Responsables	Ingeniero de Datos
Procedimiento	1. **PipeLine:** Crear flujos automatizados para extraer los datos periódicamente. 2. **Depuración:** Eliminar duplicados, corregir nulos y estandarizar formatos.. 3. **Versionamiento:** Guardar una "foto" del dataset usado para garantizar reproducibilidad. 4. **Aprobar:** Ingeniero de Datos aprueba DataSet.
Entregable estandarizado	Dataset Limpio y Versionado (Training Set).

Tabla 12. Ficha de implementación operacional del elemento Seguridad

Elemento	Seguridad
Objetivo	Garantizar la confidencialidad, integridad y disponibilidad de los datos y del modelo durante todo el ciclo.
Criterio de Aplicación	Transversal (aplica en todo momento, pero se revisa en cada pase a producción).
Roles Responsables	CISO (Oficial de Seguridad) y DevSecOps.
Procedimiento	1. **Control de Acceso:** Implementar control de acceso según rol para que solo personal autorizado vea los datos o el código. 2. **Defensa:** Proteger los activos tecnologicos del framework. 3. **Aprobar:** Oficial de Seguridad aprueba la seguridad de la información aplicada.
Entregable estandarizado	Certificado de Seguridad

Tabla 13 – Ficha de implementación operacional del elemento elección de Algoritmos

Elemento	Elección de Algoritmos
Objetivo	Seleccionar y diseñar la arquitectura matemática o modelo más adecuado para resolver el problema.
Criterio de Aplicación	Una vez que los datos están listos.
Roles Responsables	Ingeniero de Datos, Ingeniero de Desarrollo
Procedimiento	1. **Experimentación:** Probar distintos algoritmos o modelos con el dataset. 2. **Ajuste:** Calibrar los hiperparámetros para maximizar la métrica de éxito. 3. **Selección:** Elegir el modelo "campeón" basándose en el equilibrio entre precisión y costo computacional. 4. **Aprobar:** Ingeniero de Datos aprueba el modelo
Entregable estandarizado	Informe de Selección de Modelo y Código del Modelo Entrenado.

Tabla 14 – Ficha de implementación operacional del elemento Despliegue de Modelos

Elemento	**Despliegue de Modelos**
Objetivo	Mover el modelo validado desde el entorno de desarrollo al entorno productivo para usuarios reales.
Criterio de Aplicación	Cuando el modelo ha pasado las pruebas de calidad (QA) y seguridad.
Roles Responsables	Ingeniero de Desarrollo / MLOps
Procedimiento	1. **Empaquetado:** Contenerizar el modelo (ej. Docker) con todas sus dependencias. 2. **Estrategia de Despliegue:** Elegir la estrategia de despliegue para minimizar riesgos. 3. **Lanzamiento:** Activar el servicio para el tráfico real. 4. **Aprobar:** Lider de Proyecto, Ingeniero de Desarrollo aprueba despliegue.
Entregable estandarizado	Modelo en Producción Activo

Tabla 15 – Ficha de implementación operacional del elemento Monitoreo y Mantención

Elemento	**Monitoreo y Mantención**
Objetivo	Vigilar la salud del modelo en el tiempo y corregir degradaciones.
Criterio de Aplicación	Continuo (24/7) desde el despliegue.
Roles Responsables	Equipo de Operaciones, Ingeniero de Datos, Ingeniero de Desarrollo
Procedimiento	1. **Observabilidad:** Recolectar logs de errores y tiempos de respuesta. 2. **Detección de Drift:** Comparar los datos reales con los de entrenamiento para detectar cambios en el comportamiento del usuario. 3. **Re-entrenamiento:** Si el rendimiento cae bajo el umbral, disparar un nuevo ciclo de entrenamiento 4. **Aprobar:** Equipo de Operaciones aprueba desempeño del modelo.
Entregable estandarizado	Dashboards de Salud del Modelo y Alertas de Re-entrenamiento.

4 Validación del Diseño del Framework

La validación de un framework orientado a la adopción responsable de inteligencia artificial en el ámbito de las telecomunicaciones requiere no solo una fundamentación teórica, sino también la verificación empírica de su aplicabilidad en contextos organizacionales reales. Con este propósito, se diseñó una encuesta estructurada que permite evaluar la pertinencia, utilidad y robustez del modelo propuesto desde la perspectiva de los potenciales usuarios y responsables de su implementación.

El instrumento se organizó en tres secciones principales:

- Toma de Decisiones Estratégicas
- Trazabilidad, Auditabilidad y Seguridad
- Eficiencia, Adquisición de Activos y Competitividad

Cada sección aborda dimensiones críticas del framework, tales como la capacidad de apoyar decisiones de inversión en IA, la transparencia y explicabilidad de los procesos, y el impacto en la optimización de recursos y la ventaja competitiva.

La encuesta utiliza una escala Likert de cinco puntos (1 = muy en desacuerdo, 5 = muy de acuerdo), lo que permite capturar percepciones cuantificables y comparables entre distintos actores de la organización. De este modo, se busca obtener evidencia empírica que respalde la validez del framework, identificando fortalezas, oportunidades de mejora y el grado de alineación con los objetivos estratégicos de la Gerencia de Operaciones.

En conjunto, este proceso de validación constituye un paso esencial para garantizar que el framework no solo cumpla con los estándares académicos y normativos, sino que también se traduzca en una herramienta práctica, confiable y auditable para la toma de decisiones en entornos de alta complejidad tecnológica.
La encuesta se distribuyó de forma digital, garantizando anonimato y voluntariedad. Considerando una muestra representativa de perfiles técnicos y estratégicos dentro de la Gerencia de Operaciones de una empresa de telecomunicaciones del pais. La estructura de la encuesta se adjunta como Anexo de esta Tesina.

4.1 Análisis de Resultados

4.1.1 Información Demográfica de los Participantes

La validación del framework contó con 12 profesionales de diversas áreas de la Gerencia de Operaciones y de Seguridad de la Información, distribuidos en seis cargos clave (**B.Tabla 1**). Esta muestra ofrece una representación equilibrada entre niveles decisionales y operativos, permitiendo contrastar el modelo desde la mirada estratégica hasta su implementación técnica. En términos etarios, los roles de mayor jerarquía (Subgerente, Gerente y Oficial de Seguridad) se concentran entre los 45 y 50 años, aportando una sólida trayectoria en liderazgo e inversión; en contraste, los perfiles técnicos (Ingenieros de Datos y de Desarrollo) se sitúan entre los 30 y 35 años, entregando una visión actualizada sobre adopción de IA, trazabilidad y algoritmos. Por su parte, los jefes de Área (35 a 45 años) actúan como puente entre la ejecución y la estrategia. En conjunto, esta composición demográfica multidisciplinaria asegura pertinencia técnica y otorga alta robustez y legitimidad a los hallazgos de la encuesta.

4.1.2 Visión Global por Dimensión

El gráfico de radar de la **B.Figura 1** sintetiza los promedios de las tres dimensiones evaluadas, evidenciando mayor consenso hacia los bordes y áreas de mejora hacia el centro. La dimensión decisiones estratégicas obtuvo la puntuación más alta (4,56), validando al framework como soporte clave para reducir la incertidumbre, gobernar iniciativas de IA y alinearlas con los objetivos de la Gerencia de Operaciones. Le sigue eficiencia, adquisición de activos y competitividad (4,51), lo que ratifica la capacidad del modelo para optimizar costos, seleccionar proveedores y aportar valor operacional. Por último, trazabilidad, auditabilidad y seguridad alcanzó 4,43; si bien se mantiene en un rango alto y confiable, de igual forma podrian explorarse mejoras.

4.1.3 Presentación Resultados por Dimensión

Los resultados obtenidos en la dimensión *Toma de decisiones estratégicas* como se muestran en la **B.Tabla 2** y **B**.**Figura 2** evidencian una valoración altamente positiva del framework por parte de los participantes, tanto en términos de utilidad práctica como de alineación con los objetivos de la Gerencia. Todos los ítems evaluados presentan promedios superiores a 4.40 en la escala Likert, con varios alcanzando valores de 4.75, lo que indica un nivel de consenso destacable. Asimismo, los porcentajes de acuerdo (respuestas 4 = De Acuerdo y 5 = Muy de acuerdo) se sitúan entre el 83% y el 100%, consolidando la percepción favorable del modelo en esta dimensión crítica.

En particular, destacan los ítems relacionados con la precisión informativa para fundamentar decisiones estratégicas (ítem 1), la alineación con los objetivos de la Gerencia de Operaciones (ítem 4), y la capacidad del framework para priorizar proyectos según impacto y viabilidad técnica (ítem 5), todos con un promedio de 4.67 o superior y un 92% de acuerdo. Estos resultados sugieren que el modelo propuesto no solo es considerado útil para la toma de decisiones, sino también en el enfoque estratégico.

Además, el ítem que evalúa la sistematización de la necesidad justificada de soluciones basadas en IA (ítem 8) alcanza un 100% de acuerdo, lo que refuerza la idea de que el framework aporta claridad y estructura en etapas tempranas del ciclo de vida de los proyectos. La capacidad del modelo para facilitar consensos entre áreas técnicas y gerenciales (ítem 7), así como para minimizar riesgos éticos y operativos (ítem 6), también recibe una valoración sólida, lo que indica que el framework contribuye a una gobernanza más integrada y responsable.

En conjunto, estos resultados muestran que el modelo es percibido como útil, confiable y pertinente para apoyar decisiones críticas en la adopción de inteligencia artificial tanto para perfiles ejecutivos como técnicos.

Los resultados obtenidos en la dimensión *Trazabilidad, Auditibilidad y Seguridad* como se muestran en la tabla **B.Tabla 3** y **B.Figura 3** reflejan una valoración sólida y transversal del framework en aspectos críticos para la adopción responsable de inteligencia artificial. La mayoría de los ítems presentan promedios superiores a 4.50 y niveles de acuerdo que alcanzan o superan el 92%, lo que indica un alto consenso respecto a la capacidad del modelo para garantizar trazabilidad de datos, cumplimiento normativo, generación de reportes técnicos y transparencia frente a stakeholders.

Destacan especialmente los ítems relacionados con la identificación de responsables (accountability), la confianza generada por la transparencia del framework y la sistematización de procesos de auditoría, todos con 100% de acuerdo. Estos resultados validan el enfoque del modelo en términos de gobernanza y control.

No obstante, los ítems vinculados a la explicabilidad para usuarios no técnicos y la documentación estandarizada presentan promedios más bajos (4.00) y menor consenso (67%), lo que sugiere oportunidades de mejora en la comunicación técnica y la formalización documental. En conjunto, esta dimensión confirma que el framework es percibido como robusto, confiable para la gobernanza de IA, con oportunidades de mejora en comunicación técnica.

Los resultados en la dimensión *Eficiencia, Adquisición de activos y competitividad* (B.Tabla 4 y B.Figura 4) evidencian una percepción altamente favorable del framework, con promedios superiores a 4,25 y niveles de acuerdo entre el 92% y el 100%. Este consenso respalda su utilidad para optimizar decisiones de compra o desarrollo (ítem 7), agilizar la evaluación de proveedores y reducir el desperdicio computacional (ítem 8). Resaltan especialmente la estandarización para el escalamiento (ítem 5), la selección de plataformas (ítem 1) y la adopción rápida de IA (ítem 3), con valoraciones de 4,58 o más y consensos del 92% al 100%.

55En conjunto, esta dimensión confirma que el framework es percibido como una herramienta eficaz para mejorar la eficiencia operativa, optimizar la gestión de activos tecnológicos y fortalecer la competitividad institucional en procesos de adopción de inteligencia artificial.

El análisis de resultados muestra que el framework es percibido como robusto, confiable y pertinente para la adopción de inteligencia artificial. Las tres dimensiones evaluadas alcanzaron promedios elevados y altos niveles de acuerdo, reflejando un consenso transversal entre perfiles ejecutivos y técnicos, los hallazgos evidencian la aplicabilidad del marco como una herramienta robusta tanto en gobernanza como en competitividad operativa, con oportunidades puntuales de mejora en explicabilidad y documentación.

5 Validación de la Hipótesis

La hipótesis central de esta tesina establece que *"La implementación de un framework de gobernanza y operación para inteligencia artificial contribuye a la mejora en la calidad de la toma de decisiones al hacerlas más informadas y auditables, facilitando el desarrollo de las soluciones con IA como la adquisición estratégica de activos tecnológicos (plataformas, datos y modelos)"*. Al revisar los resultados obtenidos a través de la encuesta permiten validar la hipótesis central de esta investigación, el framework propuesto es percibido como una herramienta útil, confiable y transversal para apoyar la adopción responsable de inteligencia artificial en entornos organizacionales. Esta afirmación se sustenta en evidencia empírica consistente, recogida a partir de la evaluación de tres dimensiones clave como es la toma de decisiones estratégicas, trazabilidad y seguridad, y eficiencia operativa por parte de un grupo diverso de profesionales que representan tanto niveles ejecutivos como técnicos dentro de la Gerencia de Operaciones.

En la dimensión toma de decisiones estratégicas, el framework alcanzó los promedios más altos (hasta 4,75 en la escala Likert) y niveles de acuerdo que llegan al 100%, lo que indica una fuerte validación de su capacidad para fundamentar decisiones críticas, reducir la incertidumbre por ejemplo en temas como retorno de la inversión u oportunidades de aplicación de la IA y alinear criterios con los objetivos de la Gerencia. Esta dimensión fue evaluada principalmente por perfiles con experiencia en liderazgo y gestión de proyectos, lo que refuerza la legitimidad de los resultados y sustenta la contribución del framework en la calidad de la toma de decisiones.

La dimensión eficiencia, adquisición de activos y competitividad también se observa una valoración destacada, con promedios superiores a 4,50 y altos niveles de acuerdo. Los participantes reconocen que el framework facilita la selección de proveedores, mejora la relación costo-beneficio y permite escalar soluciones de IA de manera más efectiva. Estos resultados evidencian que el modelo no solo aporta valor estratégico, sino también operacional, siendo útil en la toma de decisiones técnicas (como adquisición de activos estratégicos) y presupuestarias. Lo cual refuerza que el framework facilita el desarrollo de soluciones con IA.

Por su parte, la dimensión trazabilidad, auditabilidad y seguridad mostró una percepción positiva, con promedios cercanos a 4,70 en ítems relacionados con cumplimiento normativo, generación de reportes y transparencia. No obstante, se identificaron oportunidades de mejora en aspectos como la explicabilidad para usuarios no técnicos y la documentación estandarizada, que obtuvieron promedios más bajos (4,00) y menor consenso (67%). Estas observaciones permiten proyectar ajustes específicos que fortalezcan la aplicabilidad del framework en contextos de gobernanza técnica y regulatoria. Estos ajustes son importantes en el entendido de facilitar el desarrollo de soluciones con IA ya que los usuarios tanto técnicos como no técnicos puedan tener claridad de lo que se está implementando.

En conjunto, los resultados reflejan un alto grado de aceptación del modelo propuesto, tanto en su diseño conceptual como en su utilidad práctica. La participación de perfiles diversos, la consistencia de los indicadores y la claridad de las respuestas permiten afirmar que la hipótesis ha sido validada con evidencia observada en una Gerencia de Operaciones de una empresa de telecomunicaciones del país. El framework demuestra ser una herramienta estratégica, auditable y eficiente, con potencial de adopción transversal en organizaciones que buscan integrar inteligencia artificial de forma responsable, alineada con objetivos operativos, normativos y éticos.

6 Conclusiones

El presente trabajo abordó la adopción de soluciones de Inteligencia Artificial en la industria de las telecomunicaciones, específicamente en una Gerencia de Operaciones, donde la ausencia de un marco normativo estructurado genera riesgos de trazabilidad, decisiones aisladas y una gestión ineficiente de activos tecnológicos.

A través del desarrollo del Framework de Gobernanza y Operación, fundamentado en los estándares ISO/IEC 42001, ISO/IEC 23894 e ISO/IEC TR 24028, se logró diseñar una solución que integra los niveles estratégicos, de gobernanza y operacionales con una aplicabilidad práctica directa para resolver los problemas abordables con IA en una Gerencia de Operaciones de la industria de las telecomunicaciones.

La validación del framework mediante la consulta a expertos y tomadores de decisiones de la Gerencia (con una escala de 1 a 5), permite concluir que:

- El framework es percibido como una herramienta altamente eficaz para alinear las iniciativas de IA con los objetivos de la Gerencia. Los resultados arrojaron un promedio de 4.75 en la capacidad del modelo para fundamentar decisiones estratégicas y un 100% de acuerdo en la sistematización de la necesidad justificada de soluciones.

- Se observó que la caracterización propuesta impacta directamente en la eficiencia operativa. El 100% de los encuestados coincidió en que el framework facilita el escalamiento de soluciones y reduce el desperdicio de recursos en pruebas fallidas.

- La hipótesis planteada al inicio de esta investigación sostenía que el framework "contribuye a la mejora en la calidad de la toma de decisiones facilitando el desarrollo de las soluciones con IA como la adquisición estratégica de activos". Esta hipótesis se acepta y valida en el contexto de casos abordados, dado que la dimensión de "Toma de decisiones estratégicas" obtuvo la valoración más alta (4.56), confirmando que el modelo reduce la incertidumbre y agiliza los tiempos de aprobación.

En resumen, el framework desarrollado logra transformar el proceso de adopción de la IA de una "caja negra" tecnológica a un activo corporativo gestionado, auditable y seguro, cumpliendo con los objetivos planteados en esta tesina.

7 Trabajo Futuro

Si bien el framework ha mostrado ser robusto en sus aspectos normativos y estratégicos, el análisis de los resultados de la validación expuso áreas de oportunidad que abren nuevas líneas de investigación y desarrollo:

Mejora en la Explicabilidad para Usuarios No Técnicos: La validación muestra que, aunque la trazabilidad técnica es alta, la "explicabilidad" de las soluciones para perfiles no técnicos obtuvo la menor puntuación (4.00) con un consenso del 67%. Un trabajo futuro debe centrarse en desarrollar capas de visualización o "traducción" de métricas de adopción de IA que permitan a los usuarios no técnicos comprender el comportamiento de los modelos sin necesidad de conocimientos profundos en ciencia de datos.

Gestión Documental: Incorporar en el framework la gestión de documentos estandarizados con el fin de convertirla en una fuente de datos que sirva como base para futuras iniciativas que se requiera cubrir con IA, sirviendo también como apoyo en el razonamiento de otros agentes o LLMS.

Adaptación a Nuevas Regulaciones (Ley de IA): Dado que el entorno regulatorio es dinámico (como la Ley de IA de la UE o normativas locales emergentes), una futura iteración de este trabajo debería incorporar módulos específicos de Compliance legal automatizado que se actualicen según la jurisdicción donde opere la empresa de telecomunicaciones.

Referencias

[1] NTT Data, "El Futuro de las Telecomunicaciones: IA, Eficiencia Operativa y Nuevos Modelos de Negocio," 2 jul. 2025. [Online]. Available: https://cl.nttdata.com/insights/blog/el-futuro-de-las-telecomunicaciones
[2] TeleSemana, "IA en telecomunicaciones: eficiencia operativa, ética y transformación digital," 2025. [Online]. Available: https://www.telesemana.com/blog/webinar/ia-en-telecomunicaciones-eficiencia-operativa-etica-y-transformacion-digital/
[3] A. Barros, "La IA y sus grandes desafíos de gobernanza," El Escritorio de Alejandro Barros, 2 sep. 2024. [Online]. Available: https://www.alejandrobarros.com/la-ia-y-sus-grandes-desafios-de-gobernanza/
[4] CENS, "Gobernanza de la IA en beneficio de la humanidad," Informe final, oct. 2024. [Online]. Available: https://cens.cl/wp-content/uploads/2024/10/governing_ai_for_humanity_final_report_es.pdf
[5] https://www.iso.org/standard/42001
[6] ISO, "ISO/IEC 42001:2023 – AI Management Systems," 2023. [Online]. Available: https://committee.iso.org/es/norma/42001
[7] AENOR, "ISO 42001 Gestión Inteligencia Artificial," 2024. [Online]. Available: https://www.aenor.com/certificacion/empresas/tecnologias-de-la-informacion/gestion-inteligencia-artificial
[8] https://www.iso.org/standard/77304.html
[9] https://www.iso.org/standard/77608.html
[10] ISO/IEC, ISO/IEC 42001:2023 – Artificial Intelligence Management Systems – Requirements, International Organization for Standardization, 2023.
[11] https://ieeexplore.ieee.org/document/9032420
[12] A. Brisett, "Governing AI responsibly with ISO/IEC 42001," NQA Blog, Sept. 2025.
[13] IEEE, IEEE Standard for an Architectural Framework for the Internet of Things (IoT), IEEE Std 2413-2019, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/9032420
[14] AcademiaLab, "ISO/IEC/IEEE 42010: Descripción de la arquitectura de sistemas y software," AcademiaLab, 2025. [Online]. Available: https://academia-lab.com/enciclopedia/isoiec-42010/
[15] https://www.iso.org/about
[16] ISO, "What is Artificial Intelligence (AI)?," International Organization for Standardization, 2023. [Online]. Available: https://www.iso.org/artificial-intelligence/what-is-ai
[17]https://www.iso.org/standard/74296.html
[18] IEEE, "Editorial: What is Artificial Intelligence?," IEEE Xplore, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9523786
[19] ISO/IEC 22989:2022, Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology, International Organization for Standardization, 2022. [Online]. Available: https://www.iso.org/standard/74296.html
[20] ICC, AI Governance and Standards: Policy Paper, International Chamber of Commerce, Jul. 2025. [Online]. Available: https://iccwbo.org/wp-content/uploads/sites/3/2025/07/2025-ICC-Policy-Paper-AI-governance-and-standards.pdf
[20] ISO/IEC, ISO/IEC 42001:2023 – Artificial Intelligence Management Systems — Requirements, International Organization for Standardization, 2023. [Online]. Available: https://www.iso.org/standard/81295.html
[21] Deloitte, "ISO 42001 Standard for AI Governance and Risk Management," Deloitte Insights, 2024. [Online]. Available: https://www.deloitte.com/us/en/services/consulting/articles/iso-42001-standard-ai-governance-risk-management.html
[22] A. Brisett, "Gobernanza responsable de la IA con ISO/IEC 42001," NQA Blog, Sept. 2025. [Online]. Available: https://www.nqa.com/es-cl/resources/blog/september-2025/governing-ai-responsibly-with-iso-iec-42001
[23] DigitalDefynd, "5 ways Verizon is using AI [Case Study]," 2025. [Online]. Available: https://digitaldefynd.com/IQ/verizon-using-ai-case-study/
[24] DigitalDefynd, "AI in Telecom [10 Success Stories]," 2025. [Online]. Available: https://digitaldefynd.com/IQ/ai-in-telecom-success-stories/
[25] TM Forum, "Autonomous Networks Toolkit," 2025. [Online]. Available: https://www.tmforum.org/resources/toolkit/autonomous-networks-toolkit/
[26] El Confidencial, "Telefónica progresa en 2025 hacia la era de las redes hiperautomatizadas," Dec. 29, 2025. [Online]. Available: https://www.elconfidencial.com/empresas/2025-12-29/telefonica-redes-automatizacion-inteligencia-cuantica-1hms_4276184/
[27] Mobile World Live, "China Mobile and Huawei unveil world's largest commercial 5G-A IntelligentRAN network," Nov. 28, 2024. [Online]. Available: https://www.mobileworldlive.com/china-mobile-and-huawei-unveil-worlds-largest-commercial-5g-a-intelligentran-network/

Anexos

A. Correspondencia conceptual y trazabilidad normativa del *framework*

Tabla 1. Correspondencia conceptual y trazabilidad normativa del *framework*

Concepto del diagrama	ISO/IEC 42001 (Sistema de Gestión IA)	ISO/IEC 23894 (Gestión de Riesgos IA)	ISO/IEC TR 24028 (Confiabilidad IA)
Estrategia de IA	Política de IA; integración en objetivos estratégicos	Riesgos estratégicos	Impacto en confiabilidad organizacional
Principios éticos	Transparencia y equidad	Riesgos éticos y regulatorios	Sesgos y explicabilidad
Políticas	Política formal de IA	Integración de riesgos	Normas de robustez
Métricas/KPIs	Indicadores de desempeño	Métricas de riesgos	Indicadores de resiliencia
Normas	Cumplimiento normativo	Guías de gestión de riesgos	Propiedades de confiabilidad
Comité de gobernanza IA	Roles y responsabilidades	Responsables de riesgos	Accountability compartida
Roles y responsabilidades	Funciones claras	Mitigación de riesgos	Seguridad y confiabilidad
Criterios de selección	Validación de iniciativas	Evaluación de riesgos	Robustez como criterio
Controles	Procedimientos de control	Controles de mitigación	Pruebas de resiliencia
Requisitos de conformidad	Evidencias de cumplimiento	Riesgos regulatorios	Validación de confiabilidad
Evaluación técnica	Validación funcional	Riesgos técnicos	Robustez de algoritmos
Evaluación de riesgos IA	Gestión de riesgos	Núcleo de la norma	Vulnerabilidades y resiliencia
Proceso de selección	Ciclo de vida de IA	Riesgos en cada fase	Confiabilidad en despliegue
Monitoreo	Supervisión continua	Riesgos emergentes	Pruebas de resiliencia
Activo organizacional	Activo gestionado	Riesgos asociados	Confiabilidad en operación

B. Análisis de Resultados

Tabla 1. Distribución demográfica de los participantes en la validación

Cargo	Cantidad (Q)	Rango Edad (años)
Gerente	1	45 - 50
SubGerente	4	45 - 50
Jefe de Area	3	35 - 45
Ingeniero de Datos	1	30 - 35
Ingeniero de Desarrollo	2	30 - 35
Oficial de Seguridad	1	45 - 50
Total	**12**	-

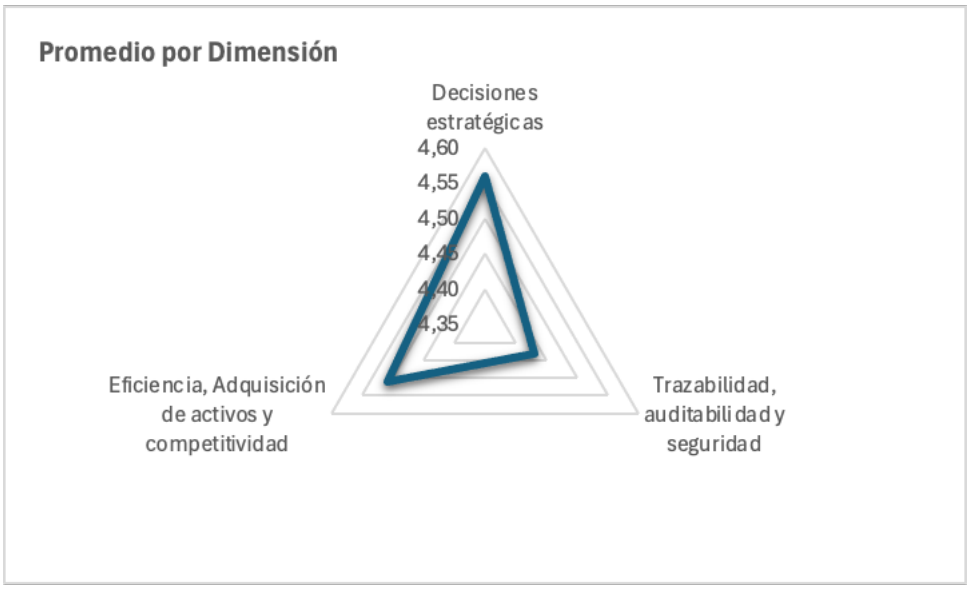


Figura 1. Valoración promedio global por dimensión del *framework*

Tabla 2. Resultados dimensión Toma de decisiones estratégicas

	Toma de decisiones estratégicas		
Item	**Enunciado**	**Promedio (Likert 1-5)**	**% de acuerdo (4-5)**
1	El framework proporciona información precisa para fundamentar decisiones estratégicas	4,75	92%
2	La implementación del framework agiliza los tiempos de aprobación de proyectos de IA	4,42	92%
3	El uso del framework reduce la incertidumbre al evaluar el retorno de inversión (ROI)	4,42	83%
4	Los criterios de decisión están correctamente alineados con los objetivos de la Gerencia de Operaciones	4,75	92%
5	El framework permite priorizar proyectos basándose en impacto y viabilidad técnica	4,67	92%
6	Las decisiones tomadas bajo este marco minimizan riesgos éticos y operativos	4,50	92%
7	El framework facilita el consenso rápido entre las áreas técnicas y las gerencias	4,42	83%
8	El framework sistematiza la determinación respecto de la necesidad (oportunidad justificada) de una solución basada en IA	4,58	100%
9	El framework sistematiza la determinación respecto de comprar o desarrollar una solución basada en IA	4,58	92%

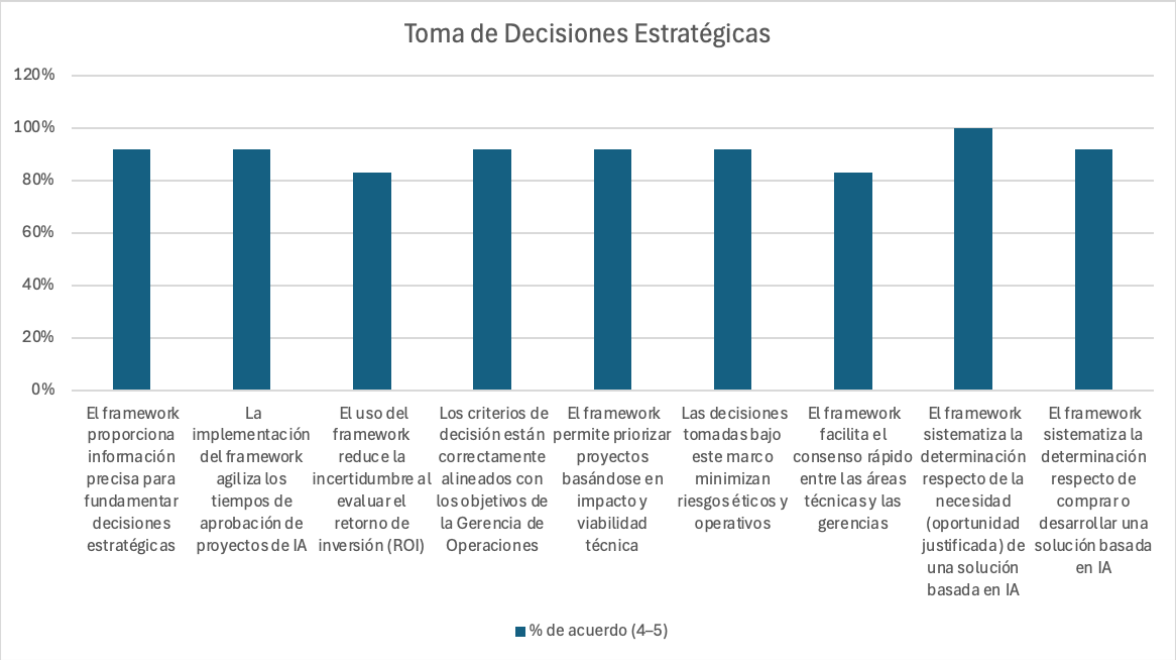


Figura 2. Gráfico resultados dimensión Toma de Decisiones Estratégicas

Tabla 3 – Resultados dimensión Trazabilidad, auditabilidad y seguridad

	Trazabilidad, auditabilidad y seguridad		
Item	**Enunciado**	**Promedio (Likert 1-5)**	**% de acuerdo (4-5)**
1	Con este framework, resulta sencillo saber exactamente de dónde provienen los datos	4,67	92%
2	El framework asegura el cumplimiento de normativas legales y leyes de privacidad	4,67	92%
3	Las soluciones de IA son explicables y comprensibles para usuarios no técnicos	4,00	67%
4	Es sencillo identificar a los responsables de cada fase (accountability)	4,58	100%
5	El framework facilita la generación de reportes técnicos para auditorías externas	4,67	92%
6	El framework permite detectar y mitigar sesgos en los resultados de los algoritmos	4,17	83%
7	Existe una documentación estandarizada que justifica el comportamiento de la IA	4,00	67%
8	El framework protege la propiedad intelectual y los activos de datos de la empresa	4,17	92%
9	La transparencia del framework aumenta la confianza de los clientes y stakeholders	4,67	100%
10	El framework sistematiza la trazabilidad y auditabilidad de los procesos de adopción de IA	4,67	92%

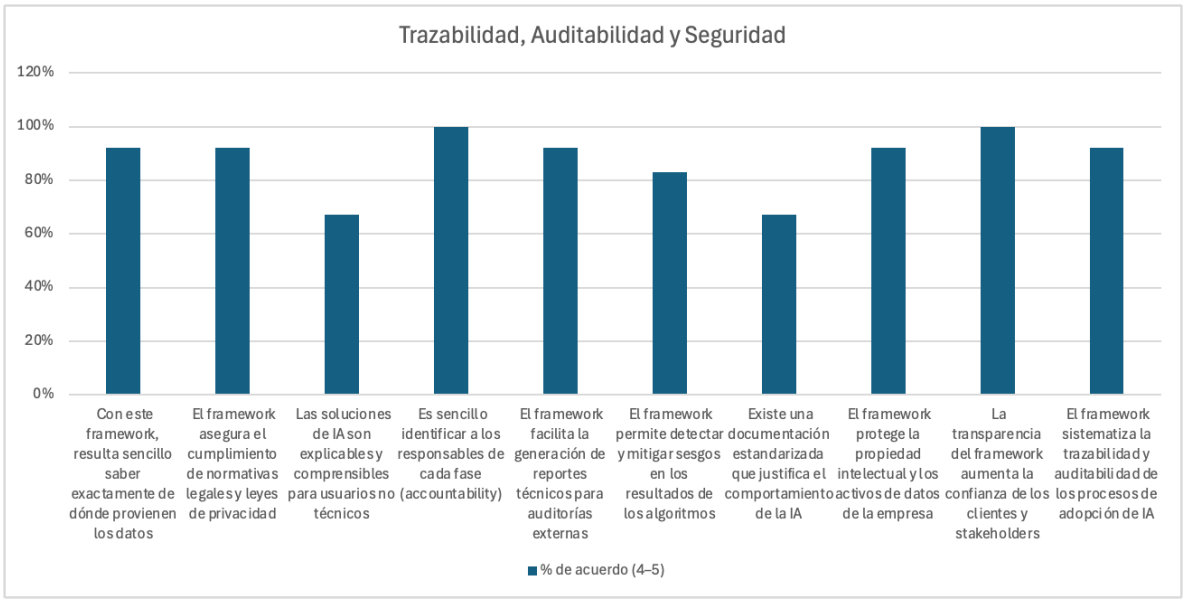


Figura 3. Gráfico resultados dimensión Trazabilidad, Auditabilidad y Seguridad

Tabla 4. Resultados dimensión Eficiencia, Adquisición de activos y competitividad

	Eficiencia, Adquisición de activos y competitividad		
Item	**Enunciado**	**Promedio (Likert 1-5)**	**% de acuerdo (4-5)**
1	El framework agiliza la evaluación y selección de proveedores y plataformas de IA	4,58	100%
2	La aplicación del framework ayuda a reducir costos innecesarios en activos tecnológicos	4,42	92%
3	El framework incrementa la competitividad al permitir una adopción de IA más rápida	4,58	92%
4	El marco de trabajo fomenta la reutilización de modelos y datos existentes	4,25	92%
5	La estandarización del framework facilita el escalamiento de las soluciones de IA	4,67	100%
6	El framework mejora la relación costo-beneficio en el desarrollo interno de soluciones	4,50	100%
7	El framework contribuye a tener claridad cuándo conviene comprar una solución hecha y cuándo es mejor fabricarla	4,58	92%
8	El framework reduce el desperdicio de recursos (cómputo, nube) en pruebas fallidas	4,50	100%
9	El framework sistematiza la adquisición y gestión de activos tecnológicos, tanto basados en IA como no	4,50	92%

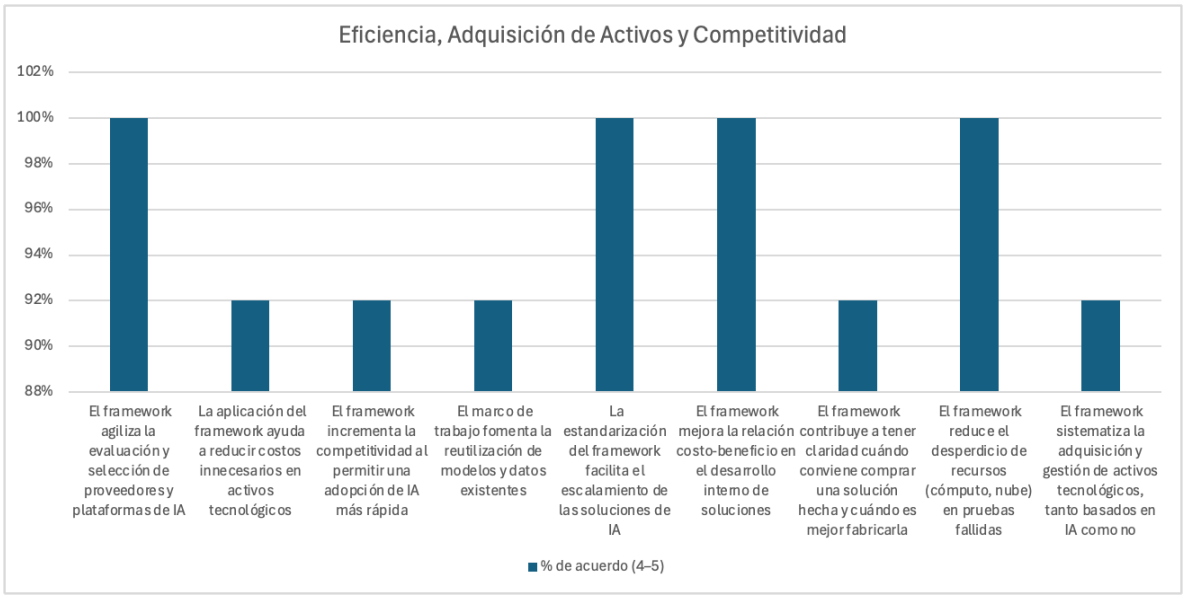


Figura 4. Gráfico resultados dimensión Eficiencia, Adquisición de activos y competitividad

C. Encuesta

Tabla 1. Estructura encuesta validación Framework

	Toma de decisiones estratégicas
1	El framework proporciona información precisa para fundamentar decisiones estratégicas
2	La implementación del framework agiliza los tiempos de aprobación de proyectos de IA
3	El uso del framework reduce la incertidumbre al evaluar el retorno de inversión (ROI)
4	Los criterios de decisión están correctamente alineados con los objetivos de la Gerencia de Operaciones
5	El framework permite priorizar proyectos basándose en impacto y viabilidad técnica
6	Las decisiones tomadas bajo este marco minimizan riesgos éticos y operativos
7	El framework facilita el consenso rápido entre las áreas técnicas y las gerencias
8	El framework sistematiza la determinación respecto de la necesidad (oportunidad justificada) de una solución basada en IA
9	El framework sistematiza la determinación respecto de comprar o desarrollar una solución basada en IA
	Trazabilidad, auditabilidad y seguridad
1	Con este framework, resulta sencillo saber exactamente de dónde provienen los datos
2	El framework asegura el cumplimiento de normativas legales y leyes de privacidad
3	Las soluciones de IA son explicables y comprensibles para usuarios no técnicos
4	Es sencillo identificar a los responsables de cada fase (accountability)
5	El framework facilita la generación de reportes técnicos para auditorías externas
6	El framework permite detectar y mitigar sesgos en los resultados de los algoritmos
7	Existe una documentación estandarizada que justifica el comportamiento de la IA
8	El framework protege la propiedad intelectual y los activos de datos de la empresa
9	La transparencia del framework aumenta la confianza de los clientes y stakeholders
10	El framework sistematiza la trazabilidad y auditabilidad de los procesos de adopción de IA
	Eficiencia, Adquisición de activos y competitividad
1	El framework agiliza la evaluación y selección de proveedores y plataformas de IA
2	La aplicación del framework ayuda a reducir costos innecesarios en activos tecnológicos
3	El framework incrementa la competitividad al permitir una adopción de IA más rápida
4	El marco de trabajo fomenta la reutilización de modelos y datos existentes
5	La estandarización del framework facilita el escalamiento de las soluciones de IA
6	El framework mejora la relación costo-beneficio en el desarrollo interno de soluciones
7	El framework contribuye a tener claridad cuándo conviene comprar una solución hecha y cuándo es mejor fabricarla
8	El framework reduce el desperdicio de recursos (cómputo, nube) en pruebas fallidas
9	El framework sistematiza la adquisición y gestión de activos tecnológicos, tanto basados en IA como no

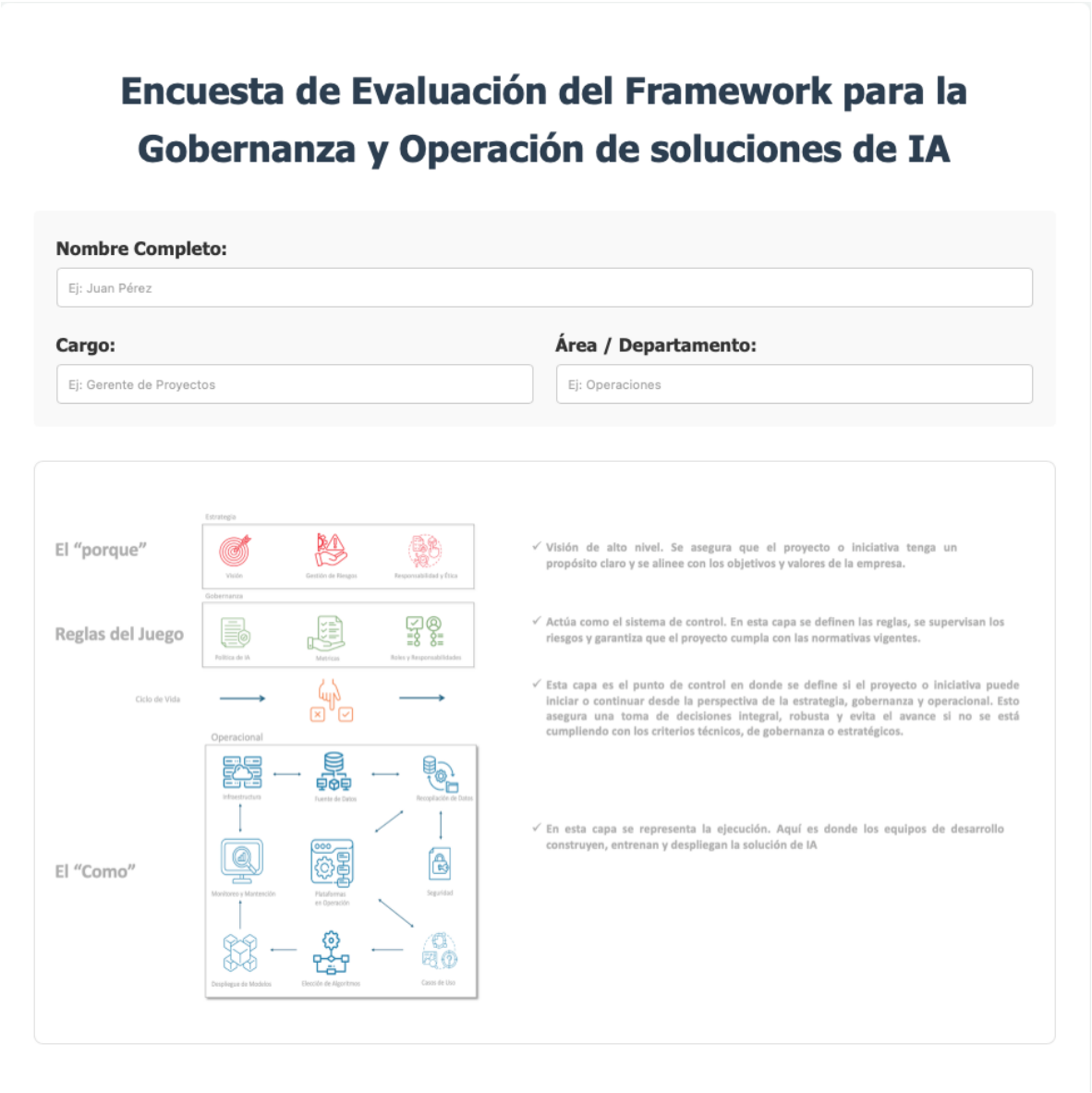


Figura 1. Formulario digital de evaluación del framework de gobernanza y operación de soluciones de IA