UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

REPÚBLICA DEL ECUADOR

UNIVERSIDAD ESTATAL DE MILAGRO

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

FACULTAD DE POSGRADOS

PROPUESTAS METODOLÓGICAS Y TECNOLÓGICAS AVANZADAS

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN TRANSFORMACIÓN DIGITAL E INNOVACIÓN

TEMA:

Percepción sobre la seguridad y ética en el uso de la inteligencia artificial en la transformación digital y propuesta de un marco de gobernanza para La Fabril S.A.

Autor:

Vélez Flores Bryan Fernando

Tutor:

Mgs. Vinueza Martínez Jorge

Milagro, 2026

Derechos de Autor

Sr. Dr.

Fabricio Guevara Viejó

Rector de la Universidad Estatal de Milagro

Presente.

Yo, **Bryan Fernando Vélez Flores,** en calidad de autor y titular de los derechos morales y patrimoniales de este informe de investigación, mediante el presente documento, libre y voluntariamente cedo los derechos de Autor de este proyecto de desarrollo, que fue realizada como requisito previo para la obtención de mi Grado, de **Magíster en Tecnologías de la Información con Mención en Transformación Digital e Innovación**, como aporte a la Línea de Investigación **Propuesta Metodológicas y Tecnologías Avanzadas** de conformidad con el Art. 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, concedo a favor de la Universidad Estatal de Milagro una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Milagro para que realice la digitalización y publicación de este Proyecto de Investigación en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Milagro, **31 de julio del 2026**

Bryan Fernando Velez Flores
Time Stamping Security Data

Bryan Fernando Vélez Flores

C.I.: 1311434961

Aprobación del Tutor del Trabajo de Titulación

Yo, **Mgs. Jorge Luis Vinueza Martínez**, en mi calidad de director del trabajo de titulación, elaborado por **Bryan Fernando Vélez Flores**, cuyo tema es **Percepción sobre la seguridad y ética en el uso de la inteligencia artificial en la transformación digital y propuesta de un marco de gobernanza para La Fabril S.A.**, que aporta a la Línea de Investigación **Propuesta Metodológicas y Tecnologías Avanzadas**, previo a la obtención del Grado **Magíster en Tecnologías de la Información con Mención en Transformación Digital e Innovación**. Trabajo de titulación que consiste en una propuesta innovadora que contiene, como mínimo, una investigación exploratoria y diagnóstica, base conceptual, conclusiones y fuentes de consulta, considero que el mismo reúne los requisitos y méritos necesarios para ser sometido a la evaluación por parte del tribunal calificador que se designe, por lo que lo **APRUEBO**, a fin de que el trabajo sea habilitado para continuar con el proceso de titulación de la alternativa de Informe de Investigación de la Universidad Estatal de Milagro.

Milagro, 31 de julio del 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JORGE LUIS VINUEZA MARTINEZ

Mgs. Jorge Luis Vinueza Martínez

C.I.: 0916860588

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

FACULTAD DE POSGRADO

ACTA DE SUSTENTACIÓN

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

En la Facultad de Posgrado de la Universidad Estatal de Milagro, a los diecisiete días del mes de agosto del dos mil veintiseis, siendo las 15:00 horas, de forma VIRTUAL comparece el/la maestrante, ING. VELEZ FLORES BRYAN FERNANDO, a defender el Trabajo de Titulación denominado **" PERCEPCIÓN SOBRE LA SEGURIDAD Y ÉTICA EN EL USO DE LA INTELIGENCIA ARTIFICIAL EN LA TRANSFORMACIÓN DIGITAL Y PROPUESTA DE UN MARCO DE GOBERNANZA PARA LA FABRIL S.A."**, ante el Tribunal de Calificación integrado por: Ph.D VINUEZA MORALES MARIUXI GEOVANNA, Presidente(a), Bach. CORREA PERALTA MIRELLA AZUCENA en calidad de Vocal; y, Phd. CHACON LUNA ANA EVA que actúa como Secretario/a.

Una vez defendido el trabajo de titulación; examinado por los integrantes del Tribunal de Calificación, escuchada la defensa y las preguntas formuladas sobre el contenido del mismo al maestrante compareciente, durante el tiempo reglamentario, obtuvo las siguientes calificaciones:

TRABAJO DE TITULACION	**60.00**
DEFENSA ORAL	**39.00**
PROMEDIO	**99.00**
EQUIVALENTE	**EXCELENTE**

Para constancia de lo actuado firman en unidad de acto el Tribunal de Calificación, siendo las 16:00 horas.

Mariuxi Geovanna Vinueza Morales
Time Stamping Security Data

PH.D VINUEZA MORALES MARIUXI GEOVANNA
PRESIDENTE/A DEL TRIBUNAL

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MIRELLA AZUCENA CORREA PERALTA

MGTI. CORREA PERALTA MIRELLA AZUCENA
VOCAL

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ANA EVA CHACON LUNA

PHD. CHACON LUNA ANA EVA
SECRETARIO/A DEL TRIBUNAL

Firmado electrónicamente por:
BRYAN FERNANDO VELEZ FLORES

VELEZ FLORES BRYAN FERNANDO
MAESTRANTE

Dedicatoria

Dedico este trabajo, en primer lugar, a Dios, por guiar mis pasos y darme la perseverancia necesaria para alcanzar esta meta. De manera muy especial a mi madre, cuyo amor incondicional y respaldo constante han sido el motor fundamental de mi vida y de mi carrera profesional. Asimismo, dedico este logro a La Fabril S.A., por la confianza depositada en mi desarrollo y por ser el excelente escenario que hizo posible esta investigación. Finalmente, a mi familia y amigos en general, por su paciencia, comprensión y apoyo invaluable a lo largo de todo este riguroso e importante proceso académico.

Agradecimientos

A la Universidad Estatal de Milagro (UNEMI), por brindarme la oportunidad de cursar mis estudios de cuarto de nivel y ponerme en el camino de la superación profesional.

De igual manera, a cada uno de los docentes de la Maestría en Tecnologías de la Información, quienes con su valiosa experiencia compartieron las bases de conocimiento que sustentan este trabajo de titulación.

Agradezco profundamente a mi tutor de tesis, Mgs. Jorge Luis Vinueza Martínez, por su valioso tiempo, sus acertadas directrices y su paciencia a lo largo de este proceso. Su guía metodológica y exigencia académica fueron fundamentales para la correcta estructuración y el éxito de esta investigación.

Asimismo, expreso mi sincera gratitud a La Fabril S.A., y de manera muy especial a las personas que participaron en este proyecto haciendo posible el diseño y la viabilidad de esta propuesta.

Finalmente, agradezco a todas las personas que, de forma directa o indirecta, me brindaron su apoyo y motivación durante el desarrollo de esta maestría. A todos ellos, mi más sincero reconocimiento.

Resumen

La presente investigación analiza la percepción sobre la seguridad y la ética en el uso de la Inteligencia Artificial (IA) en La Fabril S.A., empresa ubicada en el cantón Montecristi, provincia de Manabí, Ecuador, con el objetivo de proponer un marco de gobernanza corporativa que mitigue las vulnerabilidades identificadas. El estudio adoptó un enfoque cuantitativo, con un diseño no experimental de corte transversal y un alcance descriptivo-correlacional. La información se recolectó mediante un cuestionario estructurado de 10 ítems con escala Likert, validado con un coeficiente Alfa de Cronbach de 0,933 (confiabilidad excelente), el cual fue aplicado a una muestra probabilística de 464 colaboradores activos, seleccionados mediante un muestreo aleatorio de un universo de 2.049 empleados. Los resultados revelaron una significativa brecha formativa en las variables de estudio: el 35,78% de la muestra presentó un nivel muy bajo de claridad ética (D1: media = 2,64), el 21,98% reportó nunca haber recibido capacitación formal (D2: media = 3,17), y un absoluto 0% alcanzó el nivel avanzado de conocimiento técnico operativo (D3: media = 2,82). La prueba de Chi-cuadrado de Pearson confirmó una relación de dependencia significativa entre el nivel de conocimiento técnico y la importancia otorgada a la prevención de riesgos ($\chi^2 = 640.53$; $gl = 12$; $p < 0,001$). A pesar de esta baja capacidad técnica, se identificó una alta conciencia del riesgo sistémico y una demanda casi total (media = 4,64; varianza = 0,31) por la creación de políticas de control. En respuesta, se diseñó el Marco de Gobernanza (MGAI-LF v1.0), que articula políticas de uso aceptable, clasificación de datos y un programa de capacitación continuo, alineado con la Estrategia Nacional de IA del Ecuador (MINTEL, 2026) y los estándares NIST AI RMF, COBIT 2019 e ISO/IEC 42001:2023.

Palabras clave: gobernanza de inteligencia artificial, alfabetización digital, ciberseguridad corporativa, ética de datos, transformación digital.

Abstract

The present research analyzes the perception of security and ethics in the use of Artificial Intelligence (AI) at La Fabril S.A., a company located in the Montecristi canton, province of Manabí, Ecuador, aiming to propose a corporate governance framework to mitigate the identified vulnerabilities. The study adopted a quantitative approach, with a non-experimental, cross-sectional design and a descriptive-correlational scope. Information was collected through a structured 10-item Likert-scale questionnaire, validated with a Cronbach's Alpha coefficient of 0.933 (excellent reliability), which was applied to a probabilistic sample of 464 active collaborators, selected through random sampling from a universe of 2,049 employees. The results revealed a significant training gap in the study variables: 35.78% of the sample showed a very low level of ethical clarity (D1: mean = 2.64), 21.98% reported never having received formal training (D2: mean = 3.17), and an absolute 0% reached an advanced level of operational technical knowledge (D3: mean = 2.82). The Pearson Chi-square test confirmed a significant dependency relationship between the level of technical knowledge and the importance given to risk prevention ($\chi^2 = 640.53$; $gl = 12$; $p < 0.001$). Despite this low technical capacity, a high awareness of systemic risk and an almost total demand (mean = 4.64; variance = 0.31) for the creation of control policies were identified. In response, the Governance Framework (MGAI-LF v1.0) was designed, which articulates acceptable use policies, data classification, and a continuous training program, aligned with the National AI Strategy of Ecuador (MINTEL, 2026) and the international NIST AI RMF, COBIT 2019, and ISO/IEC 42001:2023 standards.

Keywords: artificial intelligence governance, digital literacy, corporate cybersecurity, data ethics, digital transformation.

Lista de Figuras

Lista de Tablas

Índice / Sumario

Introducción

En el transcurso de las últimas décadas, la transformación digital y la incorporación de tecnologías disruptivas han sido motivo de numerosas investigaciones en el ámbito organizacional, existiendo un creciente interés por desarrollar mejores formas de integrar la Inteligencia Artificial (IA) en los procesos de negocio para potenciar la productividad y la competitividad, habiéndose logrado avances importantes en la optimización de recursos, la automatización de decisiones y la gestión del conocimiento corporativo.

Para entender la adopción ética de esta tecnología, es importante citar a (Podevin et al., 2026), quienes dentro de la literatura científica de Springer y Scopus destacan que la era de la IA exige una profunda reflexión ética que balancee la innovación con la responsabilidad corporativa, definiendo que los marcos de confianza de TI deben asegurar el resguardo de la privacidad del usuario, la transparencia de los algoritmos y la prevención de usos inmorales de los datos personales. Asimismo, en el entorno de la transformación digital empresarial (Galarza-Sánchez et al., 2023), complementan que la IA generativa actúa como un potente catalizador de eficiencia, pero advierten que su adopción efectiva requiere obligatoriamente un enfoque estratégico ético soportado por capacidades de gobernanza y marcos normativos específicos que garanticen su uso seguro, responsable e inclusivo.

Particularmente en el sector manufacturero e industrial de gran escala, al igual que con otras tecnologías de la información, se viene procurando incluir estas herramientas de automatización en los procesos de negocio diarios, lo que ha sido sumamente de gran beneficio; sin embargo, la falta de una gobernanza formal y la baja alfabetización digital del personal operativo dejan ver que, en la actualidad, el uso ético y seguro de la Inteligencia Artificial en el entorno laboral es una realidad a

medias. A nivel mundial, desde que fue proclamada la Recomendación sobre la Ética de la Inteligencia Artificial por la UNESCO en el año 2021, muchos países asumieron el compromiso de estructurar lineamientos de control que protejan la privacidad de los individuos y garanticen un desarrollo informático confiable.

En el Ecuador, a partir del inicio de la presente década, se dio un paso trascendental para la regulación del ecosistema digital corporativo. El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), mediante el Acuerdo Ministerial MINTEL-2025-0030 publicado el 19 de enero de 2026, emitió la *Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en Ecuador (2025–2029)* (Deloitte, 2026); ante este hito histórico nacional, los análisis legales de Deloitte Ecuador constatan que, esta estrategia establece un marco de gobernanza responsable que exige a las organizaciones del sector privado revisar y actualizar con carácter de obligatoriedad sus políticas internas, especialmente en materia de privacidad, gobernanza de datos, seguridad de la información y capacitación de su personal para garantizar un uso seguro y responsable.

Todo ello ha cobrado una vigencia crítica en las organizaciones ecuatorianas en los últimos años, donde según cifras publicadas por El Telégrafo (Telégrafo, 2025), el 40% de las empresas en Ecuador ya ha implementado de forma activa soluciones basadas en IA en su operatividad diaria. No obstante, este veloz despliegue tecnológico sin una gobernanza adecuada ha provocado que aumente el índice de vulnerabilidad digital en el país. De acuerdo con los datos oficiales de la Fiscalía General del Estado, entre enero de 2022 y mayo de 2025 se receptaron un total de 20,602 denuncias por ciberdelitos a nivel nacional, de las cuales el 57% (11,833 casos) correspondieron al delito de apropiación fraudulenta por medios electrónicos (Moreira Mera, 2025). Este alarmante escenario demuestra la indefensión de los sistemas organizacionales y la urgencia de establecer políticas de respuesta rápidas frente a la suplantación de

identidad, la interceptación ilegal de datos y el acceso no consentido a sistemas corporativos.

En el contexto específico de La Fabril S.A., la problemática estudiada se manifiesta a través de diversas vulnerabilidades prácticas que replican un patrón de riesgo global. Si bien la organización ha provisto de acceso oficial a herramientas corporativas avanzadas como Gemini, la falta de políticas reguladoras y de programas formativos disminuye el impacto de esta medida de seguridad. Los colaboradores interactúan diariamente con herramientas en la nube e IA generativa de uso personal sin supervisión del departamento de TI; este fenómeno, denominado en la literatura científica como *Shadow AI* (IA en la sombra), ha sido documentado por Deloitte (Fineberg et al., 2025), quienes señalan que hasta un 69% de los empleados utiliza herramientas personales para propósitos laborales de manera silenciosa. Las causas de esta situación en la empresa se alinean con los hallazgos europeos de Deloitte (Deloitte, 2024), donde se constata que la falta de capacitación hace que el 38% de los colaboradores no logre identificar riesgos de seguridad al ingresar información en sistemas no autorizados. Esta asimetría formativa, la ausencia de directrices claras sobre qué tipo de propiedad intelectual (como recetas de producción o fórmulas de costos) se permite procesar de forma segura en el entorno corporativo de Gemini, y la falta de un marco de gobernanza de TI, exponen a una organización de gran escala como La Fabril S.A. a riesgos inminentes de exfiltración involuntaria de datos confidenciales, emulando incidentes históricos de fuga de información como el ocurrido en la multinacional Samsung (Ray, 2023).

Analizando todo ello, se determinó la importancia de realizar un trabajo de investigación orientado a diseñar una propuesta de marco de gobernanza de Inteligencia Artificial para La Fabril S.A., que incorpore políticas de control de seguridad de la información y un programa de capacitación en ética digital para los

colaboradores, lo que se considera sumamente importante pues aporta una solución real y oportuna para mitigar la vulnerabilidad informática empresarial y dar cumplimiento a la estrategia nacional de IA del Ecuador, a la vez que desde el punto de vista social e institucional se protege la privacidad de los datos personales y se promueve una cultura organizacional proactiva, segura y responsable.

Para ello y considerando lo expuesto anteriormente, se desarrolló el trabajo de tesis que a continuación se presenta, en el cual se muestra en el Capítulo I el planteamiento de la problemática, los objetivos metodológicos, las hipótesis estadísticas del estudio y la operacionalización de las variables; seguidamente, el Capítulo II recopila los antecedentes científicos y las bases teóricas de la gobernanza algorítmica; el Capítulo III detalla el marco metodológico, la determinación de la muestra probabilística y el instrumento de recolección de datos; el Capítulo IV presenta el análisis descriptivo y correlacional, la varianza de consenso y la comprobación de hipótesis; el Capítulo V expone la discusión académica de los hallazgos en contraste con la literatura, las limitaciones identificadas, conclusiones y recomendaciones finales; y finalmente, el Capítulo VI presenta la propuesta del marco de gobernanza corporativa para la organización.

CAPÍTULO I: El Problema de la Investigación

1.1. Planteamiento del problema

En el transcurso de las últimas décadas, se ha notado un incremento bastante significativo en la adopción de herramientas basadas en Inteligencia Artificial (IA) dentro de los procesos diarios de transformación digital corporativa a nivel global, lo que tal vez no se deba únicamente a una necesidad instrumental de automatización de tareas, sino a que con el pasar del tiempo, se ha priorizado la integración de la analítica avanzada, la optimización de recursos y la toma de decisiones estratégicas dentro de la planificación de las grandes empresas (Galarza-Sánchez et al., 2023; Podevin et al., 2026).

Por otra parte, es importante destacar que a nivel latinoamericano, puntualmente en las dos últimas décadas se viene promoviendo la transformación digital y la incorporación de infraestructuras de tecnologías de la información (TI) en el sector industrial, lo que ha generado un mayor desarrollo operativo, pero a su vez mayores complicaciones en la seguridad de la información corporativa, debido a que en los entornos laborales en los que se introduce esta tecnología, suele existir una severa ausencia de directrices de gobernanza de datos y de las condiciones necesarias para su control y mitigación oportuna ante incidentes cibernéticos (Sistema Económico Latinoamericano y del Caribe (SELA), 2025).

En la provincia de Manabí, de forma específica en el complejo industrial de la empresa La Fabril S.A. ubicado en el cantón Montecristi, los procesos de transformación tecnológica han facilitado el acceso corporativo formal a herramientas avanzadas como Gemini; no obstante, la interacción diaria de los colaboradores con estos sistemas no resulta del todo segura. El personal administrativo y operativo carece de los conocimientos técnicos y de la claridad ética necesarios para el manejo asertivo de estos algoritmos, desconocimiento que genera una falta de estrategias y de

medidas de precaución con las cuales proteger la privacidad y confidencialidad de la información corporativa, provocando que los empleados ingresen datos reservados (como recetas de producción, fórmulas de costos o proyecciones financieras) en servidores públicos de terceros sin la debida supervisión de TI, lo que acarrea un riesgo inminente de fuga de propiedad intelectual, exposición a ciberdelitos e incidentes de seguridad que emulan casos históricos de filtración de información ocurridos en multinacionales de escala global Samsung (Ray, 2023).

Esto genera una problemática importante de abordar, pues es en el ecosistema de la transformación digital donde se forman las bases necesarias para que las organizaciones continúen desarrollando sus operaciones y estrategias competitivas en los niveles subsiguientes del mercado; esta es una etapa en la que posee una relevancia notable la evaluación del comportamiento conductual de los usuarios, puesto que es el factor humano el que define la eficacia de las barreras de ciberseguridad corporativas frente a las amenazas informáticas, habiendo demostrado prestigiosas consultoras de seguridad global que el analfabetismo digital y la falta de directrices éticas internas elevan exponencialmente el riesgo y el costo financiero derivado de la exfiltración de bases de datos confidenciales en las compañías Deloitte e IBM (Fineberg et al., 2025; IBM Security, 2025).

Muchos de los colaboradores involucrados en la automatización de procesos manifiestan un notable interés por el uso de herramientas inteligentes de IA, por lo que resulta viable analizar la percepción de esta tecnología como un elemento clave para la optimización de los flujos de trabajo; sin embargo, para que los líderes de TI puedan identificar las brechas de seguridad latentes, es indispensable examinar cómo interactúa el conocimiento de los colaboradores frente a su capacidad operativa para detectar riesgos, un aspecto que actualmente representa uno de los mayores desafíos y vacíos de estudio en la industria manufacturera nacional.

Todo ello motiva a la realización del presente trabajo de investigación, el cual es llevado a cabo con la finalidad de aportar evidencia científica en el área de la gobernanza de tecnologías de la información, analizando cada una de las causas que inciden en la subestimación del riesgo digital en La Fabril S.A. y estudiando la problemática a fondo desde una perspectiva explicativa. El estudio se justifica ante la necesidad científica de comprender por qué la información sensible de las empresas muchas veces se encuentra expuesta en la red, identificando si la brecha de alfabetización digital y la falta de claridad ética del personal son las causas directas que impiden un resguardo asertivo de los activos intangibles de la organización.

Por tanto, se considera indispensable diagnosticar científicamente la interacción de los colaboradores con los sistemas de IA en La Fabril S.A., evaluando estadísticamente la influencia de la capacitación formal en la mitigación de vulnerabilidades informáticas, lo que permitirá generar un nuevo conocimiento empírico aplicable que contribuya a comprender los desafíos de la ciberseguridad corporativa bajo un entorno guiado por las exigencias éticas y normativas de la estrategia nacional del Ecuador.

1.2. Delimitación del problema

La delimitación de la investigación se estructuró bajo cuatro dimensiones fundamentales que acotan el alcance y la viabilidad del estudio:

- **Delimitación Temática:** El estudio se circunscribe al campo de la Gobernanza de Tecnologías de la Información, la ciberseguridad corporativa y la ética de datos, evaluando específicamente la percepción sobre la seguridad y el riesgo en el uso de la Inteligencia Artificial.

- **Delimitación Espacial**: La investigación se llevó a cabo físicamente en las instalaciones del Complejo Industrial de la empresa La Fabril S.A., ubicado en el cantón Montecristi, provincia de Manabí, Ecuador.

- **Delimitación Temporal:** El levantamiento de información y el análisis de la problemática abarcan el período comprendido entre los años 2025 y 2026, coincidiendo con la emisión de la Estrategia Nacional de Inteligencia Artificial del MINTEL (Deloitte, 2026).

- **Delimitación Poblacional:** El universo de análisis comprendió al personal activo de La Fabril S.A. (N = 2049 colaboradores), evaluando de manera representativa a una muestra probabilística de n = 464 participantes.

1.3. Formulación del problema

A partir de la problemática y el contexto analizados en los apartados previos, se plantea el siguiente problema de investigación:

¿De qué manera la brecha de alfabetización digital y la ausencia de directrices éticas inciden en la subestimación de los riesgos de seguridad derivados del uso de la Inteligencia Artificial en los procesos de transformación digital de La Fabril S.A.?

1.4. Preguntas de investigación

Para segmentar de manera lógica y dar respuesta progresiva al problema general formulado, se plantearon las siguientes preguntas de investigación que delimitan el curso metodológico del estudio:

1. ¿Cuál es el nivel actual de conocimiento técnico, claridad ética y percepción de riesgos de ciberseguridad y privacidad que poseen los colaboradores de La Fabril S.A. frente al uso de la Inteligencia Artificial?

2. ¿De qué manera influye el nivel de alfabetización digital de los colaboradores de La Fabril S.A. en su capacidad operativa para identificar vulnerabilidades de ciberseguridad asociadas al uso de la Inteligencia Artificial?
3. ¿Qué políticas de control de seguridad de la información, lineamientos éticos corporativos y componentes formativos deben estructurar el diseño de una propuesta de marco de gobernanza de Inteligencia Artificial adaptada a La Fabril S.A.?

1.5. Objetivos

1.5.1 Objetivo general

Analizar la percepción sobre la seguridad y ética en el uso de la Inteligencia Artificial en los procesos de transformación digital de La Fabril S.A. y diseñar una propuesta de marco de gobernanza corporativa que garantice una adopción tecnológica ética, segura y responsable.

1.5.2 Objetivos específicos

- Diagnosticar el nivel de conocimiento técnico, la claridad ética y los riesgos percibidos de ciberseguridad y privacidad por parte de los colaboradores de La Fabril S.A. frente al uso de la Inteligencia Artificial.
- Evaluar la relación estadística entre el nivel de alfabetización digital de los colaboradores y su capacidad para identificar vulnerabilidades operativas en la organización mediante análisis correlacional.
- Diseñar una propuesta de marco de gobernanza de Inteligencia Artificial para La Fabril S.A., que incorpore: (a) políticas de uso aceptable de herramientas de IA, (b) lineamientos de clasificación y

protección de datos, y (c) un programa modular de capacitación en ética digital para los colaboradores.

1.6. Hipótesis

Considerando el alcance correlacional e inferencial de la investigación y la necesidad de comprobar empíricamente la relación de dependencia entre las variables de estudio, se procedió a la formulación de las siguientes hipótesis de trabajo:

1.6.1 Hipótesis General (Hg):

A mayor nivel de conocimiento y alfabetización digital, mayor y más rigurosa será la percepción crítica y responsable de los colaboradores frente a la evaluación de riesgos éticos y de seguridad en el uso de Inteligencia Artificial en La Fabril S.A.

1.6.1.1 Hipótesis Nula (H0):

No existe una relación estadísticamente significativa entre el nivel de conocimiento técnico de los colaboradores de La Fabril S.A. y la importancia otorgada a la evaluación de riesgos de la Inteligencia Artificial en los procesos de transformación digital.

1.6.1.2 Hipótesis Alternativa (H1):

Existe una relación estadísticamente significativa entre el nivel de conocimiento técnico de los colaboradores de La Fabril S.A. y la importancia otorgada a la evaluación de riesgos de la Inteligencia Artificial en los procesos de transformación digital.

1.7. Justificación

Desde una perspectiva teórica, la importancia de este estudio radica en su contribución al estado del arte sobre la gobernanza algorítmica en entornos corporativos manufactureros de América Latina, un sector donde la literatura científica suele priorizar soluciones de ciberseguridad puramente técnicas, relegando a un segundo plano el análisis del factor humano. Al correlacionar científicamente la alfabetización digital con la percepción responsable del riesgo, esta investigación llena un vacío de información empírica, sirviendo de base conceptual para futuros investigadores interesados en la intersección entre la ética de la información y la adopción de tecnologías de Inteligencia Artificial.

En el plano metodológico, la justificación se sustenta en el diseño y la validación estadística de un cuestionario estructurado de alta consistencia interna. La solidez de este instrumento métrico, respaldada por la evaluación de una muestra probabilística representativa de 464 colaboradores, dota a la comunidad académica y al sector empresarial ecuatoriano de una herramienta estandarizada y replicable para medir la madurez digital y el nivel de preparación ética de los usuarios antes del despliegue de sistemas algorítmicos complejos.

Desde el punto de vista social e institucional, la utilidad de la investigación se evidencia en su potencial para beneficiar de forma directa a la alta gerencia, a los líderes de TI y al departamento de Recursos Humanos de La Fabril S.A. El diagnóstico resultante proporciona una hoja de ruta empírica para la toma de decisiones, permitiendo enfocar los recursos formativos de manera eficiente y diseñar políticas internas que protejan la privacidad de los datos personales. Socialmente, el estudio promueve un entorno de trabajo ético, inclusivo y transparente, fomentando una cultura de supervisión humana y concienciación que salvaguarda los derechos digitales de los colaboradores

en pleno proceso de transición tecnológica corporativa.

1.8. Declaración de las variables (Operacionalización)

Para el desarrollo metodológico del estudio, se procedió en primera instancia a la declaración de las variables de investigación, definiéndolas de la siguiente manera:

- **Variable Independiente (V.I.):** Nivel de alfabetización y conocimiento técnico, entendida como la frecuencia de capacitación formal recibida por el colaborador y el dominio auto-reportado de las medidas de precaución y principios éticos frente al uso de la Inteligencia Artificial.
- **Variable Dependiente (V.D.):** Percepción crítica y responsable, referida al nivel de capacidad operativa del colaborador para identificar vulnerabilidades y el grado de importancia otorgada a la evaluación de riesgos éticos y de seguridad digital en la organización.

1.8.1 Matriz de operacionalización de variables

Con la finalidad de transformar estos conceptos teóricos en elementos medibles y contrastables para la comprobación de hipótesis, se estructuró la matriz de operacionalización detallada a continuación (véase Tabla 1):

Tabla 1 *Matriz de Operacionalización de Variables*

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA	ÍTEM DEL CUESTIONARIO
Variable Independiente: **Nivel de alfabetización y conocimiento técnico**	Grado de formación y dominio conceptual que posee el colaborador respecto al uso ético, seguro y responsable de herramientas de IA en su entorno laboral.	Se mide a través de: (1) claridad sobre principios éticos, (2) frecuencia de capacitación formal recibida, y (3) nivel de conocimiento sobre medidas de precaución.	**D1. Claridad ética**	• Nivel de comprensión de los principios éticos que rigen el uso de IA. • Conocimiento de los límites del uso corporativo de IA.	**Ordinal / Likert** 1 = Muy Bajo 2 = Bajo 3 = Medio 4 = Alto 5 = Muy Alto	**Ítem 1:** "¿Cuál es su nivel de claridad sobre los principios éticos básicos que deben guiar el uso de herramientas de IA en sus funciones?"
			D2. Frecuencia de capacitación	• Regularidad con la que el colaborador recibe formación en ética y seguridad digital. • Cobertura del programa de capacitación corporativa.	**Ordinal / Likert** 1 = Nunca 2 = Rara vez 3 = Ocasionalmente 4 = Frecuentemente 5 = Muy frecuentemente	**Ítem 4:** "En su formación profesional o interna, ¿con qué frecuencia ha recibido capacitación sobre ética y seguridad digital para utilizar la IA de forma responsable?"
			D3. Conocimiento técnico operativo	• Dominio de medidas de precaución aplicables al uso de IA en procesos diarios. • Referencia: ningún colaborador alcanzó el nivel Muy Alto (0%).	**Ordinal / Likert** 1 = Muy Bajo 2 = Bajo 3 = Medio 4 = Alto 5 = Muy Alto	**Ítem 5:** "¿Cuál es su nivel de conocimiento exacto sobre las medidas de precaución que debe aplicar al utilizar IA en sus procesos diarios?"
Variable Dependiente: **Percepción crítica y responsable**	Capacidad del colaborador para identificar, valorar y reaccionar responsablemente ante los riesgos éticos y de seguridad derivados del uso de IA en el entorno laboral.	Se mide a través del nivel auto-reportado de: percepción de riesgo, capacidad de identificar vulnerabilidades, importancia de evaluación de riesgos, preocupación por sesgos, valoración de supervisión humana, conciencia del riesgo sistémico y demanda de políticas.	**D4. Percepción de riesgo de ciberseguridad**	• Nivel de riesgo asociado al uso de IA en el entorno laboral. • Identificación de amenazas de fuga de datos.	**Ordinal / Likert** 1 = Muy Bajo 2 = Bajo 3 = Medio 4 = Alto 5 = Muy Alto	**Ítem 2:** "¿Qué nivel de riesgo de ciberseguridad y fuga de datos asocia usted al uso de herramientas de IA en el entorno laboral?"
			D5. Capacidad para identificar vulnerabilidades	• Habilidad para detectar cuándo el uso de IA compromete la privacidad o confidencialidad corporativa. • Capacidad operativa de defensa ante riesgos de información.	**Ordinal / Likert** 1 = Muy Bajo 2 = Bajo 3 = Medio 4 = Alto 5 = Muy Alto	**Ítem 3:** "¿Cuál es su nivel de capacidad para identificar cuándo el uso de una IA podría comprometer la privacidad o confidencialidad de la información corporativa?"

D6. Importancia de la evaluación de riesgos	• Grado de importancia atribuida a la evaluación crítica de riesgos éticos y de seguridad antes de implementar IA. • Variable clave para la comprobación de hipótesis (Chi-cuadrado con Ítem 5).	**Ordinal / Likert** 1 = Nada importante 2 = Poco importante 3 = Neutral 4 = Importante 5 = Muy importante	**Ítem 6:** "¿Qué grado de importancia le otorga a la necesidad de evaluar críticamente los riesgos de seguridad y ética antes de implementar cualquier nueva herramienta de IA en La Fabril?"
D7. Preocupación por sesgos y errores algorítmicos	• Preocupación ante la posibilidad de que la IA sin lineamientos genere errores, sesgos o decisiones injustas. • Conciencia de las implicaciones éticas y reputacionales de la automatización.	**Ordinal / Likert** 1 = Tot. en desacuerdo 2 = En desacuerdo 3 = Ni/ni 4 = De acuerdo 5 = Tot. de acuerdo	**Ítem 7:** "Me preocupa que el uso de IA sin lineamientos corporativos claros pueda generar errores operativos, sesgos o decisiones injustas en los procesos de la empresa."
D8. Valoración de la supervisión humana	• Frecuencia con que se considera necesaria la validación humana de decisiones automatizadas. • Adherencia al enfoque 'human-in-the-loop'.	**Ordinal / Likert** 1 = Nunca 2 = Rara vez 3 = Ocasionalmente 4 = Frecuentemente 5 = Siempre	**Ítem 8:** "¿Con qué frecuencia cree que toda solución automatizada con IA dentro de la empresa debe contar con supervisión o validación humana?"
D9. Conciencia del riesgo sistémico	• Reconocimiento de que adoptar IA sin gestión de seguridad incrementa la vulnerabilidad organizacional. • Responsabilidad compartida ante la ciberseguridad corporativa.	**Ordinal / Likert** 1 = Tot. en desacuerdo 2 = En desacuerdo 3 = Ni/ni 4 = De acuerdo 5 = Tot. de acuerdo	**Ítem 9:** "Pienso que adoptar herramientas de IA sin una adecuada gestión de seguridad informática aumenta significativamente la vulnerabilidad de los sistemas de La Fabril."
D10. Demanda de políticas de gobernanza	• Nivel de acuerdo con el establecimiento de políticas corporativas explícitas para el uso seguro y ético de la IA. • Ítem con mayor consenso del estudio: varianza = 0,30.	**Ordinal / Likert** 1 = Tot. en desacuerdo 2 = En desacuerdo 3 = Ni/ni 4 = De acuerdo 5 = Tot. de acuerdo	**Ítem 10:** "Estoy a favor de que La Fabril establezca, documente y difunda políticas o protocolos explícitos sobre el uso permitido, ético y seguro de la IA."

Nota. La escala de medición es de tipo ordinal (escala Likert de 5 niveles) para todos los ítems evaluados en el instrumento (N = 464). Los ítems 5 y 6 fueron utilizados en la prueba no paramétrica de Chi-cuadrado de Pearson ($\chi^2 = 640{,}53$; $gl = 12$; $p < 0{,}001$) para la comprobación de hipótesis.

CAPÍTULO II: Marco Teórico Referencial

2.1. Antecedentes Referenciales

La comprensión de la interacción entre el capital humano y las tecnologías basadas en Inteligencia Artificial (IA) exige el análisis de investigaciones previas que delimiten el comportamiento de estas variables en entornos organizacionales contemporáneos.

Antecedentes Internacionales

A nivel internacional, la literatura científica más reciente indexada en Scopus evidencia que la asimetría entre el despliegue de herramientas de IA y la preparación técnica de los usuarios es una preocupación de escala global. En este contexto, Mariani et al. (2026) desarrollaron un estudio empírico de alto impacto enfocado en analizar la percepción que poseen los profesionales de proyectos respecto a la importancia de la alfabetización en IA (*AI literacy*) frente a las competencias tradicionales técnicas y conductuales. Mediante la aplicación de la metodología Q con profesionales de la gestión, los autores identificaron una preocupante realidad: de los cuatro perfiles de competencias analizados en las organizaciones, el enfoque orientado a la alfabetización en IA y el dominio de datos resultó ser el menos desarrollado y el menos valorado por los empleados en su práctica diaria. Este hallazgo es fundamental para la sustentación teórica del presente estudio, ya que demuestra que los colaboradores no perciben la alfabetización tecnológica como un elemento central para el éxito operativo inmediato, lo que explica por qué interactúan de manera intuitiva con herramientas algorítmicas sin medir el impacto de sus acciones.

Por su parte, Arroyo et al. (2026) aportaron una perspectiva crítica al analizar el impacto transformador de la integración tecnológica en la sostenibilidad corporativa, contrastando la visión de la gerencia frente a la de los colaboradores. A través de una revisión sistemática de la literatura y un análisis bibliométrico (2020–2025), los investigadores evidenciaron que, si bien el 70% de los ejecutivos reporta incrementos inmediatos en la eficiencia tras incorporar IA, el personal operativo experimenta una constante tensión caracterizada por la necesidad de una readecuación de competencias (*workforce reskilling*) y el temor a la obsolescencia laboral. Los autores concluyen que el éxito de la transformación digital depende del diseño de programas de capacitación que aborden el desarrollo ético y de confianza, destacando que el compromiso de la alta gerencia es el pilar indispensable para guiar a los colaboradores en esta transición, lo que valida teóricamente la necesidad de integrar comités y políticas de control institucionalizadas en las organizaciones.

Complementando este enfoque conductual, Sing et al. (2026) llevaron a cabo una investigación cuantitativa de diseño transversal con el objetivo de revelar cómo influye el uso de herramientas de IA y la capacitación formal de los colaboradores en la eficiencia laboral. Mediante un análisis de mediación aplicado a una muestra de profesionales, se demostró estadísticamente que, aunque el uso frecuente de herramientas de IA mejora la velocidad operativa, es la capacitación formal en IA la que ejerce el efecto positivo más robusto sobre el desempeño laboral y la mitigación de riesgos de ciberseguridad. El estudio concluye que las organizaciones que ejecutan programas formales de alfabetización y entrenamiento en IA registran niveles más altos de conciencia situacional frente a las vulnerabilidades, lo que reduce la propensión de los colaboradores a incurrir en prácticas inseguras, justificando por qué la capacitación es una variable indispensable para el uso seguro de estas

tecnologías en los flujos diarios de trabajo.

Finalmente, Zhu y Abd Rozan (2026) realizaron una investigación cualitativa de casos múltiples fundamentada en los marcos teóricos de la Aceptación Tecnológica (TAM) y de Tecnología-Organización-Entorno (TOE), analizando la implementación práctica de la IA en empresas del sector comercial. Los hallazgos de las entrevistas semiestructuradas revelaron que la integración de la IA ha abarcado la totalidad de la cadena de valor operativa; sin embargo, la investigación constató que la mayoría de estos procesos no opera de forma autónoma, sino bajo un modelo de colaboración denominado "preprocesamiento de la IA + ajuste y supervisión humana". El estudio concluye de forma contundente que la capacidad organizativa de la empresa y la alfabetización digital de los empleados constituyen las dos variables críticas que definen el éxito o fracaso de la adopción tecnológica, advirtiendo que las organizaciones que despliegan estas herramientas sin marcos de control o políticas de gobernanza exponen de forma constante sus sistemas a graves amenazas de ciberseguridad y pérdida de confidencialidad de la información.

Antecedentes Nacionales

Al trasladar el análisis al contexto de la República del Ecuador, la relación entre la transformación digital, el uso de la Inteligencia Artificial y la seguridad de la información corporativa adquiere una relevancia crítica debido a los recientes cambios normativos e institucionales del país. Durante los últimos años, el Estado ecuatoriano ha buscado normar la transición tecnológica, reconociendo que el despliegue acelerado de la IA en el sector empresarial exige salvaguardas éticas y legales indispensables para proteger la privacidad de los ciudadanos y la soberanía de los datos organizacionales.

En el plano de las políticas públicas, el hito más significativo se consolidó con la emisión del Acuerdo Ministerial MINTEL-2025-0030 por parte del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), mediante el cual se expidió la *Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en Ecuador (2025–2029)*. Al respecto, el análisis legal e institucional desarrollado por Deloitte (2026) señala que esta directriz nacional establece por primera vez un marco regulatorio de cumplimiento obligatorio para el sector privado que utiliza o implementa de manera activa sistemas de IA, demandando a las corporaciones nacionales la adopción de principios de transparencia, ciberseguridad por diseño, supervisión humana y mitigación de riesgos. Deloitte advierte que el cumplimiento de esta normativa obliga perentoriamente a las empresas a revisar y actualizar sus códigos de conducta internos y sus políticas de TI, garantizando que el personal posea el nivel de alfabetización digital y la claridad ética necesarios para procesar información sin vulnerar la Ley Orgánica de Protección de Datos Personales, lo que fundamenta la importancia del diseño de la propuesta para La Fabril S.A. (Deloitte, 2026).

No obstante, esta exigencia de gobernanza corporativa en el Ecuador colisiona de forma directa con una realidad caracterizada por una adopción apresurada de la IA frente a altos índices de inseguridad digital en la región andina. Por un lado, las estadísticas publicadas por El Telégrafo (2025) demuestran que el 40% de las empresas ecuatorianas ya ha integrado soluciones basadas en IA generativa en su operatividad diaria. Por otro lado, este despliegue tecnológico sin una gobernanza adecuada ha provocado un notable incremento en los incidentes de ciberseguridad a nivel regional. Al respecto, el análisis sistemático de Torres Gamarra y Zúñiga Carnero (2025) sobre las brechas estructurales en América Latina evidencia que la

rápida digitalización sin madurez institucional expone a las organizaciones a constantes amenazas informáticas, destacando que el analfabetismo digital es la principal causa de la vulnerabilidad de las empresas frente a fraudes y exfiltraciones de bases de datos. Esta vulnerabilidad se manifiesta claramente en el contexto local; de acuerdo con el consolidado oficial de denuncias de la Fiscalía General del Estado analizado por Moreira Mera (2025), el país acumuló un total de 20,602 denuncias formales por delitos informáticos, de las cuales el 57% (11,833 casos) correspondieron al delito de apropiación fraudulenta por medios electrónicos.

Estos antecedentes demuestran que las empresas en el Ecuador operan en un ecosistema digital de alta vulnerabilidad. El secuestro de información sensible (*ransomware*) y los ataques de ingeniería social (*phishing*) encuentran un vector de entrada directo en la falta de conocimiento técnico y en la baja percepción de riesgo de los colaboradores (Deloitte, 2024). En una corporación de gran envergadura como La Fabril S.A., este vacío formativo facilita que el personal cargue involuntariamente bases de datos reservadas en plataformas públicas de *Shadow AI* (IA en la sombra) buscando agilizar sus tareas, comprometiendo propiedad intelectual, fórmulas industriales y recetas de producción. Este escenario nacional valida empíricamente por qué es indispensable evaluar la alfabetización digital para diseñar un marco de gobernanza interna que proteja los activos intangibles de la organización.

Al contrastar las investigaciones de carácter internacional con la realidad ecuatoriana, se visibiliza una importante laguna en el conocimiento científico actual. Aunque existe abundante literatura científica enfocada en las dimensiones puramente técnicas de la ciberseguridad o en los marcos regulatorios estatales a nivel macro, se evidencia una notable escasez de estudios empíricos locales que analicen de qué manera la alfabetización digital y la claridad ética influyen directamente en la percepción

individual del riesgo y en la prevención de conductas inseguras (como el *Shadow AI*) dentro de la industria manufacturera andina. Por consiguiente, esta investigación viene a llenar este vacío empírico mediante el diagnóstico detallado de las percepciones operativas en La Fabril S.A., dando cumplimiento sistemático a los objetivos específicos primero y segundo planteados en este estudio.

2.2. Marco Conceptual

2.2.1 Variable Independiente: Nivel de alfabetización y conocimiento técnico

La variable de entrada, definida como el nivel de alfabetización y conocimiento técnico del personal, se refiere a la capacidad de un individuo para comprender, evaluar y aplicar de forma técnica las medidas de seguridad y principios de uso de las tecnologías emergentes en su entorno laboral. Bajo los nuevos paradigmas corporativos, esta variable se descompone en tres dimensiones de control técnico formativo:

D1. Claridad ética

La claridad ética en las funciones laborales constituye el nivel de comprensión teórica y práctica que posee el colaborador sobre las implicaciones morales, la responsabilidad en el tratamiento de datos y los límites normativos que deben guiar el uso de herramientas inteligentes. En este ámbito de formación, Chee et al. (2024) proponen un marco de competencias para la alfabetización en IA (*AI Literacy*), argumentando que la conciencia ética no debe ser tratada como un

concepto abstracto, sino como una competencia técnica e indispensable para el desarrollo del capital humano. De manera complementaria, Chen y He (2026) señalan que esta sensibilidad ética debe ser entendida como una competencia operativa que le permite al empleado identificar cuándo una acción tecnológica infringe los estándares de responsabilidad o transparencia de la organización. La falta de este indicador impide que el personal desarrolle una sensibilidad proactiva frente a dilemas como el sesgo algorítmico o la opacidad del procesamiento automático.

D2. Frecuencia de capacitación

Esta dimensión mide la regularidad, la cobertura y el alcance de los programas de instrucción formal y entrenamiento continuo que la empresa provee a sus colaboradores en materia de ciberseguridad, ética de datos y uso seguro de herramientas disruptivas. Desde la perspectiva de Sing et al. (2026), la capacitación tecnológica no debe limitarse a una inducción esporádica; por el contrario, requiere ser un proceso estructurado y adaptado a las tipologías de tareas de los empleados. La frecuencia formativa actúa como el principal mediador para elevar las competencias cognitivas del usuario, reduciendo de manera significativa la tasa de errores operativos por impericia técnica o subestimación del riesgo.

D3. Conocimiento técnico operativo

El conocimiento técnico operativo se define como el dominio real y auto-reportado que posee el colaborador respecto a las medidas de precaución y protocolos de seguridad física e informática aplicables al

interactuar con sistemas inteligentes. Zhu y Abd Rozan (2026) argumentan que este conocimiento abarca desde saber identificar una conexión segura hasta comprender cómo las plataformas públicas recopilan y almacenan los datos de entrada (*prompts*). La ausencia de esta competencia operativa genera una brecha formativa latente que impide al personal diferenciar entre herramientas de IA públicas (que entrenan algoritmos con sus datos) y versiones corporativas seguras, facilitando prácticas de alto peligro informático.

2.2.2 Variable Dependiente: Percepción crítica y responsable

La variable de salida, definida como la percepción crítica y responsable de los colaboradores, representa el nivel de conciencia de riesgo frente a vulnerabilidades, la importancia atribuida a proteger los datos confidenciales y la actitud proactiva de supervisión sobre los sistemas automatizados. Bajo el diseño metodológico de la investigación, esta variable se descompone en siete dimensiones conductuales y de control:

D4. Percepción de riesgo de ciberseguridad

La percepción de riesgo de ciberseguridad constituye la capacidad cognitiva del colaborador para identificar, evaluar y asociar posibles amenazas de vulnerabilidad digital o fuga de datos con el uso diario de herramientas tecnológicas. Como señalan Diro et al. (2025), en el entorno laboral moderno, la adopción de modelos de IA generativa incrementa exponencialmente los vectores de ataque informático, tales como la interceptación de flujos de datos o el secuestro de información.

Al respecto, Torres Gamarra y Zúñiga Carnero (2025) exponen que la baja percepción de riesgo individual de los colaboradores es el principal detonante para la proliferación del fenómeno de *Shadow AI* (IA en la sombra), ya que el usuario, al no percibir de manera inmediata la gravedad de la amenaza informática, tiende a interactuar de forma imprudente con herramientas públicas e inseguras en la nube. De este modo, una percepción de riesgo madura y proactiva actúa como la primera línea de defensa de la organización, permitiéndole al empleado reconocer que la tecnología no está exenta de peligros.

D5. Capacidad para identificar vulnerabilidades

Esta dimensión se define como la habilidad técnica y operativa que posee el colaborador para detectar de manera oportuna situaciones o acciones específicas que puedan comprometer la privacidad de los datos personales o la confidencialidad de los activos intangibles de la empresa. Según Oyebisi y Orim (2026), esta capacidad defensiva no se limita al conocimiento de las amenazas, sino al desarrollo de destrezas prácticas en el puesto de trabajo. El empleado debe ser capaz de determinar con precisión qué tipo de información corporativa y operativa sensible puede ser procesada de forma segura dentro de las plataformas autorizadas de la organización y cuál debe ser restringida para evitar su exposición.

D6. Importancia de la evaluación de riesgos

La importancia otorgada a la evaluación de riesgos representa el grado de valoración ética y preventiva que el colaborador atribuye a la necesidad de analizar críticamente los peligros informáticos antes de incorporar o interactuar con cualquier nueva solución algorítmica. De acuerdo con Alsudais (2026), esta evaluación previa constituye un pilar de la prudencia tecnológica corporativa, indispensable para anticipar contingencias legales y operativas. Asimismo, Xiong et al. (2026) señalan que las organizaciones que formalizan este tipo de evaluaciones preventivas reducen drásticamente el nivel de riesgo de sus proyectos y optimizan su toma de decisiones. Esta dimensión es de vital relevancia en la investigación, dado que constituye la variable dependiente clave que se asocia estadísticamente con el nivel de conocimiento técnico del personal, respondiendo de forma directa al segundo objetivo específico del estudio.

D7. Preocupación por sesgos y errores algorítmicos

La preocupación por sesgos y errores algorítmicos mide el nivel de conciencia y la inquietud del personal respecto a la posibilidad de que un sistema automatizado de IA, al operar de manera autónoma, genere fallas operativas, interpretaciones imprecisas o decisiones injustas dentro de los flujos de trabajo corporativos. Ishag et al. (2026) argumentan que la opacidad inherente a los algoritmos de caja negra exige que los profesionales desarrollen un pensamiento crítico y una constante supervisión ética, reconociendo que los modelos de IA son

creaciones humanas falibles que pueden heredar sesgos o distorsionar la realidad operativa de la empresa.

D8. Valoración de la supervisión humana

Esta dimensión evalúa el nivel de acuerdo del colaborador con la necesidad de que toda solución o decisión automatizada mediante Inteligencia Artificial cuente de forma obligatoria con un proceso de validación y control ejercido por un profesional humano. Zhu y Abd Rozan (2026) constatan que la integración corporativa de la IA exige la adopción del enfoque cooperativo "humano en el ciclo" (*human-in-the-loop*), donde la tecnología actúa como un elemento de preprocesamiento, pero el juicio crítico, el control ético y la decisión final recaen de forma ineludible en el operador, garantizando que el sistema no opere de manera descontrolada.

D9. Conciencia del riesgo sistémico

La conciencia del riesgo sistémico se refiere al reconocimiento formal por parte de la plantilla de que la adopción de tecnologías de IA sin una adecuada gestión de seguridad informática aumenta significativamente la vulnerabilidad de toda la red informática de la empresa. Diro et al. (2025) explican que la seguridad digital no debe ser entendida como un departamento aislado de la compañía, sino como una responsabilidad compartida de carácter sistémico, donde el comportamiento descuidado de un solo colaborador puede comprometer la continuidad operativa de toda la corporación. En este plano, la investigación sistemática de Torres Gamarra y Zúñiga Carnero (2025) sobre las brechas

estructurales en América Latina demuestra que la ciberseguridad conductual es altamente sensible; la ausencia de una conciencia sistémica del riesgo en la plantilla hace que los colaboradores asuman de forma errónea que la protección perimetral depende únicamente de los sistemas de TI, invisibilizando que un acceso no consentido o un correo de *phishing* puede paralizar de forma masiva los servicios informáticos de toda la organización.

D10. Demanda de políticas de gobernanza

La demanda de políticas de gobernanza representa el nivel de apoyo y la actitud proactiva de los colaboradores a favor de que la empresa establezca, documente y difunda de manera obligatoria directrices y protocolos explícitos sobre el uso seguro, permitido y ético de la Inteligencia Artificial. Deloitte (2024) señala que la existencia de políticas de TI formales y de carácter ético responde a una necesidad unificada del propio personal, quienes buscan en la normativa corporativa un refugio de seguridad jurídica y operativa frente a la velocidad de la transición tecnológica, permitiéndoles interactuar con sistemas de IA dentro de un marco de confianza y legalidad institucional.

En síntesis, la conceptualización detallada de estas diez dimensiones (D1 a D10) proporciona la precisión terminológica indispensable para estructurar las variables independiente y dependiente de la investigación. Al definir formalmente los indicadores que guiarán el levantamiento de información, este marco conceptual viabiliza el cumplimiento del primer objetivo específico, orientado al diagnóstico

situacional de los colaboradores, y del segundo objetivo específico, enfocado en evaluar de manera estadística e inferencial las relaciones de dependencia mediante el análisis correlacional de los datos en la organización.

2.3. Marco Teórico

2.3.1 Teoría de la Gobernanza de TI y Sistemas de Inteligencia Artificial

La inserción de la Inteligencia Artificial en los procesos de transformación digital empresarial ha obligado a la comunidad científica a reevaluar los cimientos del gobierno tradicional de Tecnologías de la Información (TI). Los modelos tradicionales de control, centrados únicamente en la infraestructura física, la capacidad de cómputo y el almacenamiento de datos, han demostrado ser insuficientes para gestionar la opacidad, autonomía y dinamismo de los sistemas de aprendizaje profundo.

En este plano, Mikkilineni y Kelly (2026) introducen una postura crítica mediante la teoría de la gobernanza de compromisos, argumentando que las operaciones de TI contemporáneas arrastran lo que denominan una "deuda de coherencia". Esta deuda se define como la acumulación de decisiones tecnológicas locales e intuitivas de los usuarios que degradan la seguridad perimetral y la auditabilidad a lo largo del tiempo, hasta ser expuestas por incidentes de seguridad o demandas regulatorias. Los autores sostienen que la gobernanza de la IA no debe limitarse a la supervisión externa de la infraestructura de cómputo, sino que debe integrar el control de la configuración, el cumplimiento de la

seguridad y el manejo ético directamente dentro de la ejecución de los procesos algorítmicos. Este enfoque teórico justifica de manera sólida por qué una corporación industrial no puede depender únicamente de barreras técnicas tradicionales, requiriendo un modelo normativo que gobierne de manera explícita el comportamiento del usuario frente a la IA.

Frente a esta necesidad de estandarización, surge a nivel internacional la norma **ISO/IEC 42001:2023** como el primer estándar mundial diseñado para establecer, implementar, mantener y mejorar de forma continua un Sistema de Gestión de Inteligencia Artificial en las organizaciones. Al respecto, Mazzinghy et al. (2025) evaluaron de manera empírica los beneficios de la adopción de este estándar en los mercados emergentes, demostrando que la implementación de este marco normativo optimiza los procesos organizacionales, mitiga significativamente los riesgos operativos y asegura que la automatización de decisiones sea éticamente auditable y transparente ante los grupos de interés. De manera complementaria, Prabha et al. (2026) analizan que la adopción de este estándar no debe realizarse de forma aislada, sino bajo un enfoque de gobernanza multicapa que unifique el sistema de gestión de seguridad de la información (ISO/IEC 27001), el de gestión de calidad (ISO 9001) y la analítica estratégica del talento humano en una única estructura de soporte para la toma de decisiones, lo que resulta de vital pertinencia para mitigar los riesgos de exfiltración de propiedad intelectual en las organizaciones.

Asimismo, Oyebisi y Orim (2026) aportan evidencia empírica clave

respecto a los desafíos de gobernanza que surgen cuando la IA se integra en la ciberseguridad corporativa. En su análisis, los autores exponen que la ocurrencia de incidentes de seguridad digital a menudo revela una severa fragmentación regulatoria dentro de las compañías, donde los comités de ciberseguridad y los líderes de desarrollo de sistemas operan de forma aislada. Para solucionar esta brecha, el estudio sugiere la imperiosa necesidad de rediseñar las estructuras organizacionales, integrando la gobernanza del ciber riesgo con un marco ético de IA bajo exigencias regulatorias internacionales estrictas (tales como la Ley de IA de la Unión Europea o la Ley Orgánica de Protección de Datos Personales en el contexto ecuatoriano), garantizando la transparencia algorítmica y la rendición de cuentas ante los directivos y grupos de interés.

Finalmente, la integración de estas corrientes da origen al diseño de la Arquitectura de Gobernanza Inteligente (AIG). Desarrollado conceptualmente por Ayoub (2026), este marco propone un modelo de gobernanza híbrido que combina la precisión analítica y predictiva de la IA con el juicio crítico, el razonamiento ético, la administración y la previsión estratégica de los seres humanos. El modelo AIG advierte que el uso de la IA a gran escala en el sector industrial introduce riesgos sistémicos de alta opacidad y concentración tecnológica, los cuales solo pueden ser gobernados de manera efectiva si el liderazgo de la compañía adopta un enfoque que subordine la optimización algorítmica a los valores institucionales de sostenibilidad, transparencia y responsabilidad ética compartida, para la propuesta de esta tesis.

2.3.1.1 Comparativa de marcos de gobernanza de inteligencia artificial internacionales

Para operativizar las teorías generales de gobernanza de TI, la práctica corporativa global ha desarrollado marcos de referencia estandarizados que guían la gestión del riesgo algorítmico. Entre los más destacados se encuentra el NIST AI Risk Management Framework (2023), el cual propone un modelo flexible, voluntario y estructurado para ayudar a las organizaciones a mapear, medir, gestionar y gobernar los riesgos asociados a las tecnologías de IA. El NIST enfatiza que un sistema de IA confiable debe ser seguro, transparente, explicable y, fundamentalmente, contar con mecanismos de rendición de cuentas y auditorías continuas.

Por otro lado, la asociación ISACA ha adaptado el marco de gobernanza de TI COBIT 2019 al dominio de la Inteligencia Artificial. Como detalla ISACA (2019), este marco no enfoca la gobernanza desde una perspectiva puramente técnica, sino desde el alineamiento estratégico del negocio, proponiendo una serie de objetivos de control específicos que aseguran que el ciclo de vida de los datos, el diseño de modelos algorítmicos y el entrenamiento de los colaboradores estén alineados con los objetivos de rentabilidad, cumplimiento legal y mitigación del riesgo empresarial.

Finalmente, el Reglamento de Inteligencia Artificial de la Unión Europea (2024) introduce la primera legislación integral y de carácter obligatorio basada en un enfoque de clasificación de riesgos (mínimo, limitado, alto e inaceptable). Esta normativa de cumplimiento obliga a las corporaciones que utilicen sistemas considerados de alto riesgo a someter sus procesos a estrictas evaluaciones de conformidad y a garantizar la total transparencia de los algoritmos ante el usuario final. Al analizar comparativamente estos tres marcos, se evidencia que una gobernanza efectiva exige la combinación del control técnico-estratégico de COBIT, el enfoque de gestión de riesgos del NIST y el cumplimiento legal del reglamento europeo, lo que responde al tercer objetivo específico del estudio al sentar las bases teóricas de la propuesta de esta investigación.

2.3.2 Enfoques y Modelos de Responsabilidad Corporativa

La integración de la Inteligencia Artificial en los procesos productivos exige una readecuación profunda de los marcos tradicionales de responsabilidad corporativa y gobierno societario. La adopción de sistemas autónomos no exime a las juntas directivas de sus obligaciones de control; por el contrario, amplía el espectro de su responsabilidad fiduciaria hacia nuevas dimensiones éticas, informáticas y operativas.

En este ámbito doctrinal, Alsudais (2026) sostiene que la introducción de la IA en la cadena de valor obliga a reformular los deberes fiduciarios

clásicos de la administración de las empresas. El autor introduce el concepto fundamental del "deber de prudencia tecnológica" (*duty of technological prudence*), el cual establece que la alta gerencia tiene la obligación legal y moral de desarrollar competencias tecnológicas y ejercer una supervisión ética rigurosa sobre los algoritmos implementados. El estudio demuestra que el uso de IA expone a las compañías a graves responsabilidades civiles y administrativas (desde fallas de ciberseguridad hasta violaciones a la privacidad de datos), por lo que propone el enfoque de "sostenibilidad por diseño" (*sustainability-by-design*) como un imperativo estratégico. Este enfoque exige que las consideraciones ambientales, de gobernanza y de protección de los derechos de los colaboradores sean embebidas a lo largo de todo el ciclo de vida del desarrollo y uso de la tecnología, proporcionando un argumento legal de gran peso para justificar el marco regulatorio propuesto en La Fabril S.A.

Desde la perspectiva de la gestión estratégica y la innovación empresarial, Xiong et al. (2026) aplican la teoría de la vista basada en la atención (*Attention-Based View*) para analizar cómo influye la atención de la alta gerencia hacia la "IA responsable" en el desempeño y la estabilidad de las organizaciones. A través de un análisis de procesamiento de lenguaje natural en conferencias de presentación de resultados financieros corporativas, los investigadores demostraron empíricamente que las empresas cuyos equipos directivos dedican una atención proactiva y constante a la responsabilidad ética de la IA generan patentes y procesos de innovación de mayor impacto y

sostenibilidad. El estudio revela que priorizar la IA responsable actúa como un activo estratégico dinámico que fomenta la inversión en capital humano especializado y mitiga significativamente los riesgos de los proyectos de innovación. Los autores sugieren que los ejecutivos deben tratar la ética de la IA como una prioridad estratégica del negocio y no como una simple tarea rutinaria de cumplimiento o legal, recomendando incorporar "puntos de control éticos" (auditorías de sesgo, revisiones de diseño seguro) en los flujos diarios de trabajo para potenciar el aprendizaje organizacional, lo que respalda de forma directa los componentes del marco propuesto en esta tesis.

Finalmente, para operativizar esta responsabilidad ética antes de que se establezcan legislaciones definitivas en los mercados, Lucas et al. (2026) proponen la necesidad de estructurar marcos de autorregulación corporativa éticamente informados. El estudio plantea que los desarrolladores y usuarios de tecnología en entornos corporativos sostienen una gran responsabilidad al transferir la IA generativa de los laboratorios al mercado. Para mitigar posibles daños y fomentar la confianza de los grupos de interés, los autores desarrollaron un marco de acción basado en definir objetivos claros, documentar procesos, evaluar sesgos, implementar controles de seguridad y fomentar la participación activa de los empleados. Este enfoque de autorregulación se complementa con la propuesta de Coovadia et al. (2025), quienes identifican cinco pilares esenciales para un gobierno corporativo ético de la IA: transparencia, mitigación del sesgo de máquina, protección de la privacidad, enfoque de IA beneficiosa e IA responsable. Ambas

corrientes teóricas coinciden en que la autorregulación ética y la gobernanza interna son herramientas indispensables para navegar el complejo paisaje moral de las tecnologías emergentes, consolidando el sustento teórico de la propuesta de esta investigación.

Por consiguiente, el “deber de prudencia tecnológica" (*duty of technological prudence*) y el enfoque de la vista basada en la atención gerencial hacia la IA responsable no deben quedar únicamente como postulados teóricos, sino que sustentan y justifican directamente el desarrollo del tercer objetivo específico del estudio: diseñar una propuesta de marco de gobernanza algorítmica y un programa modular de capacitación corporativa para La Fabril S.A.

2.3.3 Paradigma de Aumento Humano frente a la Automatización

El despliegue de la Inteligencia Artificial en los procesos corporativos ha reactivado un profundo debate ético y antropológico respecto al diseño de los sistemas tecnológicos en el entorno laboral. Frente a la tendencia tradicional de la automatización ciega, que busca reemplazar de forma total la acción humana para reducir costes, emerge con fuerza el paradigma del aumento humano, el cual sostiene que la tecnología debe ser diseñada y gobernada para complementar, expandir y potenciar las capacidades cognitivas de los colaboradores, asegurando que el control de las decisiones críticas permanezca bajo el juicio humano.

En el plano del control de procesos de negocio, Zhu y Abd Rozan (2026) constatan que, a pesar de los notables avances en las capacidades de generación y predicción de la IA, el éxito de su integración empresarial depende de la adopción del enfoque

cooperativo "humano en el ciclo" (*human-in-the-loop*). Bajo este esquema, la tecnología actúa únicamente como un elemento de preprocesamiento, procesamiento masivo y filtrado de datos, mientras que la supervisión, el ajuste fino y la toma de decisiones finales recaen de manera ineludible en el operador. Esta postura teórica coincide con los hallazgos de Ishag et al. (2026), quienes afirman que el auge de la IA generativa obliga a los profesionales a transitar desde roles puramente ejecutores y operativos hacia tareas de alta dirección que demandan pensamiento crítico, juicio de valor y sentido de responsabilidad ética. Ambos autores demuestran que la IA no debe sustituir las capacidades estratégicas humanas, sino aumentarlas, requiriendo un marco de gobernanza interna que dicte cómo debe estructurarse este modelo de colaboración híbrido para evitar la pérdida de control perimetral.

Desde una perspectiva filosófica y de ética de la virtud, Scherz (2025) advierte sobre las graves implicaciones antropológicas de un diseño tecnológico orientado al reemplazo absoluto de la fuerza laboral. El autor argumenta que la automatización total no solo amenaza con generar desempleo, sino que provoca una preocupante pérdida de competencias prácticas (*deskilling*) y elimina importantes oportunidades para el desarrollo de la virtud y la autonomía del colaborador en su puesto de trabajo. Para mitigar esta desprofesionalización, el estudio propone adoptar de forma rigurosa la teoría del aumento humano, demostrando que el uso de la IA como una herramienta de soporte que expande la acción del operador permite que el personal desarrolle

virtudes como la prudencia y el discernimiento crítico. El autor concluye que la ética tecnológica debe trascender el mero cumplimiento regulatorio para involucrarse en el diseño práctico de la tecnología dentro del espacio de trabajo, justificando científicamente por qué la propuesta de capacitación y el marco de gobernanza para La Fabril S.A. deben priorizar el empoderamiento y la educación digital del usuario frente a la automatización invasiva.

Finalmente, este paradigma debe comprenderse como una estrategia de resistencia organizacional frente a las presiones del mercado tecnológico global. En un análisis crítico de los discursos tecnocapitalistas, Méndez y Gutiérrez (2025) examinan cómo la noción de la "seguridad y alineación de la IA" (*AI safety*) está siendo a menudo cooptada por intereses corporativos para justificar una aceleración digital inevitable que margina la soberanía de los usuarios y reduce los controles éticos a meros gestos performativos. Los investigadores advierten que la opacidad y la falta de control sobre los algoritmos generan un riesgo inminente de delegación cognitiva de responsabilidades por parte del personal, lo que degrada el pensamiento crítico y la autonomía operativa de la empresa. En consecuencia, la investigación llama a una "alineación pedagógica y organizacional" de la tecnología, donde las organizaciones actúen de manera proactiva, estableciendo marcos de gobernanza y programas formativos continuos que subordinen el desarrollo tecnológico a los principios de soberanía corporativa, capacitación activa y supervisión del capital humano, consolidando de forma definitiva la necesidad

metodológica de la propuesta que desarrolla esta investigación.

2.3.4 Posicionamiento Teórico-Ideológico de la investigación

A partir del análisis crítico de las diversas corrientes doctrinales expuestas en este capítulo, la presente investigación asume un posicionamiento teórico-ideológico de carácter socio-técnico, fundamentado de manera principal en el paradigma del aumento humano y la supervisión activa (*human-in-the-loop*), en convergencia con los enfoques contemporáneos de la gobernanza corporativa de tecnologías de la información. Este posicionamiento rechaza categóricamente la visión tecnocrática e instrumentalista de la "automatización por reemplazo", la cual tiende a considerar al capital humano únicamente como un factor de coste sustituible o como el eslabón más débil y propenso al error dentro de la infraestructura digital. Por el contrario, se defiende de forma vehemente la postura de Scherz (2025), quien sostiene que la tecnología debe ser gobernada para expandir, complementar y elevar las capacidades del trabajador, preservando su autonomía cognitiva, su profesionalización y su capacidad para desarrollar la virtud y el discernimiento crítico dentro del espacio laboral.

En consecuencia, el diseño de la propuesta que desarrolla esta investigación se ampara conceptualmente en el modelo de colaboración híbrida expuesto por Zhu y Abd Rozan (2026), asumiendo que los sistemas de Inteligencia Artificial en La Fabril S.A. deben operar bajo un esquema de preprocesamiento analítico condicionado de manera obligatoria a la validación, criterio y control ético final del operador

humano. Para operativizar esta visión conductual frente a los riesgos del entorno, se adopta el enfoque de gobernanza multicapa propuesto por Prabha et al. (2026), el cual unifica el control técnico de la ciberseguridad con la capacitación ética y la concienciación de los recursos humanos. Esta fusión teórica permite al investigador justificar científicamente que la mitigación de vulnerabilidades informáticas y la erradicación del *Shadow AI* (IA en la sombra) no se lograrán únicamente mediante barreras informáticas restrictivas, sino a través de un marco de gobernanza corporativa que eduque éticamente al personal y alinee sus procesos con la estrategia nacional del Ecuador (Deloitte, 2026). Con este posicionamiento, el estudio establece una base científica sólida para la propuesta del Capítulo VI, demostrando que la seguridad de la información es un pilar estratégico indisociable de la dignidad y la capacitación activa del colaborador.

2.4. Síntesis integradora de las corrientes teóricas y su articulación metodológica

Para finalizar el Capítulo II, se presenta un análisis de síntesis integradora que unifica las tres grandes corrientes teóricas analizadas (la Gobernanza de TI, la Responsabilidad Corporativa y el Paradigma de Aumento Humano) y demuestra su alineación con los objetivos y las variables de la investigación. El marco referencial de esta tesis no se concibe como un conjunto de teorías aisladas, sino como un engranaje científico interconectado.

En primer lugar, la teoría de la gobernanza de TI y los estándares internacionales de la norma ISO/IEC 42001, COBIT 2019 y el NIST Framework proveen el soporte metodológico y normativo de control. Esta corriente se

conecta de forma directa con la variable independiente (Nivel de alfabetización y conocimiento técnico) y el primer objetivo específico, orientado a diagnosticar los niveles de claridad ética y capacitación de los colaboradores. La teoría demuestra que es imposible exigir cumplimiento regulatorio si la organización carece de una infraestructura formativa y de directrices técnicas claras.

En segundo lugar, los enfoques de responsabilidad corporativa y el "deber de prudencia tecnológica" de Alsudais (2026) establecen la justificación fiduciaria y la toma de decisiones directivas. Esta corriente se articula con la variable dependiente (Percepción crítica y responsable) y el segundo objetivo específico, el cual busca evaluar de manera estadística e inferencial de qué manera influye la alfabetización en la capacidad del personal para evitar vulnerabilidades de seguridad de la información. La teoría sustenta que los directivos de las organizaciones tienen la responsabilidad fiduciaria de velar por que sus empleados utilicen herramientas tecnológicas de forma segura.

Finalmente, el paradigma de aumento humano y la supervisión activa (*human-in-the-loop*) de Scherz (2025) y Zhu y Abd Rozan (2026) actúan como el puente de diseño práctico del estudio. Esta corriente teórica rechaza la automatización por reemplazo y fundamenta de manera contundente la necesidad del tercer objetivo específico: el diseño del marco de gobernanza corporativa y el programa de capacitación modular. De este modo, la síntesis teórica e ideológica del estudio se consolida como el plano de ingeniería social que guiará el desarrollo de la propuesta en el Capítulo VI, garantizando que la transformación digital en las organizaciones sea un proceso ético, seguro, eficiente y respetuoso de la dignidad del capital humano.

CAPÍTULO III: Diseño Metodológico

3.1. Tipo y diseño de investigación

La presente investigación se adscribió al paradigma positivista y adoptó un enfoque cuantitativo. De acuerdo con Hernández-Sampieri et al. (2014), este enfoque se caracteriza por recolectar datos estructurados para probar hipótesis a través de la medición numérica y el análisis estadístico, lo que permite establecer patrones de comportamiento. Dicho enfoque fue idóneo para el estudio, ya que se orientó a medir y cuantificar el nivel de conocimiento técnico y la percepción de riesgo de los colaboradores mediante un instrumento estandarizado, para luego comprobar las relaciones entre las variables con pruebas inferenciales.

El diseño de la investigación fue no experimental y de corte transversal. Se consideró no experimental porque no se realizó una manipulación deliberada de las variables; por el contrario, se observó el fenómeno en su contexto natural dentro de la organización, sin intervención del investigador. Asimismo, el estudio fue de corte transversal, puesto que la recolección de los datos se efectuó en un único momento, durante el período comprendido entre los años 2025 y 2026.

Finalmente, el estudio tuvo un doble alcance: descriptivo y correlacional. El alcance descriptivo permitió diagnosticar el estado actual de las diez dimensiones (D1 a D10) de las variables de estudio, detallando la distribución de sus frecuencias. Por su parte, el alcance correlacional se utilizó para evaluar científicamente la relación de dependencia estadística entre el nivel de conocimiento técnico de los colaboradores y la importancia que otorgan a la

evaluación de riesgos, permitiendo así la verificación de la hipótesis general de investigación.

3.2. Población y muestra

Población

La población objeto de estudio estuvo constituida por la totalidad de los colaboradores activos $(N = 2.049)$ de la empresa La Fabril S.A., pertenecientes al Complejo Industrial ubicado en el cantón Montecristi, provincia de Manabí, Ecuador. La caracterización poblacional incluyó al personal de los perfiles operativo, técnico y administrativo que interactúa con herramientas tecnológicas durante su jornada laboral.

Muestra

Para el cálculo del tamaño de la muestra representativa, se aplicó la fórmula de Cochran (1977) para poblaciones finitas:

$$n = \frac{n_0}{1 + \frac{n_0 - 1}{N}}$$

Donde n_0 representa el tamaño de la muestra para una población de tamaño infinito, calculado a través de la siguiente relación matemática:

$$n_0 = \frac{Z^2 \cdot p \cdot q}{e^2}$$

Para el procesamiento del cálculo muestral se adoptaron los siguientes parámetros metodológicos estándar:

- Un nivel de confianza del 95%, lo que equivale a un valor crítico de la distribución normal de $(Z = 1{,}96)$.
- Una proporción de ocurrencia del fenómeno de $(p = 0{,}50)$ y una proporción de no ocurrencia de $(q = 0{,}50)$, maximizando el tamaño de

la muestra ante la falta de antecedentes del valor poblacional.

- Un margen de error máximo admitido del 4% $(e = 0{,}04)$, el cual es altamente exigente para investigaciones en el ámbito organizacional.

Al aplicar los valores paramétricos en la fórmula de Cochran:

$$n_0 = \frac{(1{,}96)^2 \cdot 0{,}5 \cdot 0{,}5}{(0{,}04)^2} = \frac{3{,}8416 \cdot 0{,}25}{0{,}0016} = 600{,}25$$

$$n = \frac{600{,}25}{1 + \frac{600{,}25 - 1}{2049}} = \frac{600{,}25}{1 + 0{,}2924} = \frac{600{,}25}{1{,}2924} \approx 464$$

Como resultado de la aplicación matemática de la fórmula para poblaciones finitas de Cochran (1977), se obtuvo una muestra probabilística representativa de exactamente $(n = 464)$ colaboradores evaluados.

Muestreo y criterios de selección

La selección de los participantes se realizó mediante un muestreo probabilístico aleatorio estratificado por área funcional (operativa, administrativa y técnica), garantizando que cada estrato de la organización estuviera representado proporcionalmente en la muestra final. Los criterios de selección definidos fueron:

- **Criterios de inclusión:** Colaboradores con contrato activo durante el período 2025-2026 que utilizaran regularmente herramientas digitales o sistemas de IA en el desempeño de sus funciones.

- **Criterios de exclusión:** Personal que se encontrara en goce de licencia, vacaciones o en período de inducción inicial al momento del levantamiento de la información.

3.3. Métodos y técnicas

Métodos de investigación

En el desarrollo de la investigación se aplicó de manera primordial el método hipotético-deductivo. De acuerdo con Hernández-Sampieri et al. (2014), este método parte de la fundamentación de premisas teóricas universales y la postulación de hipótesis de trabajo, para posteriormente contrastar de forma empírica dichas hipótesis mediante la recolección, medición y análisis estadístico de los datos obtenidos en un entorno particular. En el presente estudio, se partió de las teorías de gobernanza de tecnologías de la información y alfabetización digital para deducir las hipótesis que correlacionan el conocimiento técnico de los colaboradores con la subestimación de riesgos cibernéticos, procediendo a su verificación cuantitativa en la organización.

Técnicas e instrumento de recolección de datos

Como técnica de recolección de información se implementó la encuesta. El instrumento de medición fue un cuestionario estructurado de 10 ítems con escala ordinal tipo Likert de cinco niveles. Los reactivos fueron diseñados para medir las diez dimensiones del marco conceptual: tres ítems evaluaron la variable independiente (Ítems 1, 4 y 5) y siete ítems la variable dependiente (Ítems 2, 3 y 6 al 10), con anclajes simétricos como "De Nunca a Siempre" o "De Muy Bajo a Muy Alto".

Validez de contenido

La validez de contenido del instrumento se determinó a través del juicio de tres expertos con grado de maestría en las áreas de TI, ciberseguridad y metodología, quienes evaluaron la suficiencia, claridad y coherencia de los reactivos. Sus sugerencias de ajuste fueron incorporadas en la versión definitiva del cuestionario.

La confiabilidad y consistencia interna de la escala fue evaluada estadísticamente mediante el coeficiente Alfa de Cronbach, obteniendo un valor de $\alpha = 0.933$. De acuerdo con George y Mallery (2003), un coeficiente superior a 0,90 demuestra una confiabilidad excelente. Este resultado validó científicamente que el instrumento midió de forma estable y coherente las variables de estudio.

Procedimiento de aplicación

La recolección de la información se llevó a cabo en las instalaciones de La Fabril S.A. aprovechando la vinculación laboral directa del investigador con la organización, lo que facilitó el acceso a la población objetivo y optimizó los tiempos de distribución del instrumento. La encuesta se administró en formato digital y de manera autoadministrada. Bajo estrictos estándares éticos, se garantizó formalmente a todos los participantes el carácter voluntario, el estricto anonimato y la confidencialidad en el tratamiento de sus respuestas, asegurando que los datos serían procesados con fines exclusivamente científicos y de forma agregada.

3.4. Procesamiento estadístico de la información

El procesamiento y análisis estadístico de los datos recolectados se estructuró en dos fases. Para la fase descriptiva (cálculo de frecuencias, medias y varianzas) y la tabulación inicial, se utilizó el software Microsoft Excel.

Para la fase inferencial, que incluyó el cálculo del coeficiente Alfa de Cronbach y la prueba de hipótesis mediante Chi-cuadrado de Pearson (χ^2), se utilizó el software de análisis de datos asistido por inteligencia artificial Julius AI. Esta herramienta fue empleada a lo largo de toda la investigación para garantizar la precisión y la correcta aplicación de los procedimientos estadísticos.

Fase descriptiva

En la primera fase, se aplicó la estadística descriptiva para caracterizar cada una de las diez dimensiones (D1 a D10) evaluadas. Para cada ítem, se calcularon las frecuencias absolutas y relativas (porcentajes), la media aritmética como medida de tendencia central y la varianza para evaluar el grado de consenso en las respuestas. Los resultados de esta fase se representaron en tablas y gráficos de barras en el capítulo siguiente.

Fase inferencial (Comprobación de hipótesis)

En la segunda fase, orientada a comprobar las hipótesis $(H_0\ y\ H_1)$, se aplicó la prueba no paramétrica de Chi-cuadrado de Pearson (x^2). Se eligió esta prueba por ser el método estadístico idóneo para evaluar la independencia entre variables categóricas de escala ordinal. El procedimiento se estructuró cruzando el Ítem 5 (Variable Independiente) y el Ítem 6 (Variable Dependiente), generando una matriz de contingencia con 12 grados de libertad (gl). Para la toma de decisiones, se adoptó un nivel de significancia de, $(\alpha = 0{,}05)$,

estableciendo que se rechazaría la hipótesis nula si el p-valor resultante fuera menor a dicho umbral.

Los grados de libertad del procedimiento se calcularon mediante la siguiente relación:

$$gl = (filas - 1) \times (columnas - 1) = (4 - 1) \times (5 - 1) = 3 \times 4 = 12$$

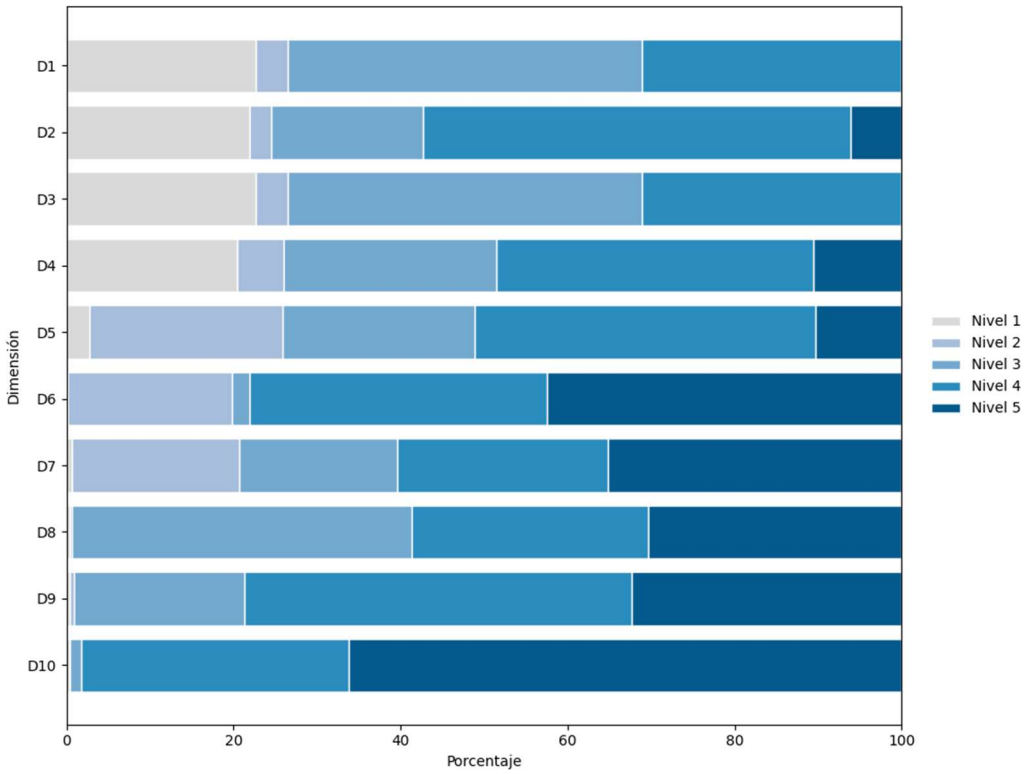
Estableciendo que el valor crítico de la distribución teórica de Chi-cuadrado para 12 grados de libertad con un nivel de confianza del 95% es de $21{,}03$, cifra que actuará como el límite matemático para determinar el rechazo de la hipótesis nula en caso de que el valor calculado en el estudio supere este umbral; de conformidad con el rigor del diseño metodológico, los resultados numéricos y la contrastación empírica resultante de este procedimiento se presentarán de forma exclusiva en el desarrollo del Capítulo IV de esta investigación de tesis.

CAPÍTULO IV: Análisis e Interpretación de Resultados

En el presente capítulo se exponen los resultados obtenidos tras la aplicación del instrumento de recolección de datos a la muestra representativa de 464 colaboradores de la empresa La Fabril S.A. La presentación de la información se estructura en tres fases: en primer lugar, se realiza un análisis descriptivo de las dimensiones evaluadas; posteriormente, se presenta la validación de la confiabilidad del instrumento; y finalmente, se expone el contraste empírico de la hipótesis de investigación mediante estadística inferencial.

A continuación, en la Figura 1, se presenta la distribución porcentual consolidada de las respuestas para las diez dimensiones evaluadas, lo que permite una visión panorámica de los resultados antes de proceder al análisis detallado de cada una.

Figura 1



Distribución porcentual por nivel de respuesta en las 10 dimensiones

4.1. Análisis e Interpretación de Resultados

En esta sección se presentan los resultados descriptivos correspondientes a las diez dimensiones (D1 a D10) que conforman las variables de estudio: Nivel de conocimiento técnico y Percepción de riesgo en el uso de Inteligencia Artificial. Los datos recolectados fueron procesados y tabulados, expresándose en frecuencias absolutas y porcentuales para facilitar su interpretación.

4.1.1 Análisis de la Dimensión 1: Claridad Ética

La Dimensión 1 evalúa la percepción de los colaboradores mediante el ítem: *"¿Cuál es su nivel de claridad sobre los principios éticos básicos que deben guiar el uso de herramientas de Inteligencia Artificial en sus funciones dentro de la empresa?"*. A continuación, en la Tabla 2, se detallan las frecuencias obtenidas:

Tabla 2

Distribución de frecuencias de la dimensión 1

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Muy bajo	166	35,78
Bajo	28	6,03
Medio	105	22,63
Alto	135	29,09
Muy alto	30	6,47
Total	**464**	**100,00**

Nota. Media = 2,64; varianza = 1,92.

La Tabla 2 presenta los resultados del Ítem 1, correspondiente a la dimensión Claridad Ética. Los hallazgos revelan que el nivel predominante en la muestra fue "Muy Bajo", con una frecuencia relativa de 35,78%, seguido por el nivel "Alto" con 29,09% de los encuestados. Estos resultados evidenciaron una preocupante polarización operativa. La media obtenida de 2,64 puntos sobre una escala de cinco niveles indica que los colaboradores de La Fabril S.A. presentan un nivel medio-bajo en esta dimensión. La varianza de 1,92 refleja una alta variabilidad y dispersión en las percepciones, lo que demostró que los principios éticos no habían sido socializados de forma estandarizada, dejando a muchos colaboradores trabajando a ciegas respecto a los lineamientos corporativos. Este resultado es coherente con lo señalado por Chee et al. (2024), quienes argumentan que la conciencia ética no debe entenderse como un concepto abstracto, sino como una competencia técnica indispensable que, al ser deficiente en una organización, evidencia una profunda brecha formativa y operativa.

4.1.2 Análisis de la Dimensión 2: Frecuencia de Capacitación

La Dimensión 2 evalúa la regularidad con la que los colaboradores han sido formados en el uso ético y seguro de la IA. Para ello, se utilizó el ítem: *"En su formación profesional o interna, ¿con qué frecuencia ha recibido capacitación sobre ética y seguridad digital para utilizar la IA de forma responsable?"*. A continuación, en la Tabla 3, se detallan las frecuencias obtenidas:

Tabla 3

Distribución de frecuencias de la dimensión 2

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Nunca	102	21,98
Rara vez	12	2,59
Ocasionalmente	84	18,10
Frecuentemente	238	51,29
Muy frecuentemente	28	6,04
Total	**464**	**100,00**

Nota. Media = 3,17; varianza = 1,63.

La Tabla 3 presenta los resultados del Ítem 4, correspondiente a la dimensión Frecuencia de Capacitación. Los hallazgos revelan que el nivel predominante en la muestra fue "Frecuentemente", con una frecuencia relativa de 51,29%, seguido por el nivel "Nunca" con 21,98% de los encuestados. Aunque más de la mitad de los colaboradores reporta recibir capacitación, existe una preocupante brecha formativa donde casi una cuarta parte de la plantilla 21,98% se encuentra completamente excluida. La media obtenida de 3,17 puntos indica un nivel general moderado en esta dimensión, pero la varianza de 1,63 refleja una dispersión moderada, evidenciando que el acceso a la formación no es homogéneo. Este resultado es coherente con los hallazgos de Sing et al. (2026), quienes demostraron que la capacitación formal es la que ejerce el efecto más robusto en la mitigación de riesgos, concluyendo que la baja frecuencia de entrenamiento en un segmento de la plantilla se traduce directamente en una menor conciencia operativa frente a las vulnerabilidades.

4.1.3 Análisis de la Dimensión 3: Conocimiento Técnico Operativo

La Dimensión 3 profundiza en el dominio práctico que poseen los colaboradores sobre las medidas de seguridad al usar IA. Para ello, se utilizó el ítem: "¿Cuál es su nivel de conocimiento exacto sobre las medidas de precaución que debe aplicar al utilizar IA en sus procesos diarios?". A continuación, en la Tabla 4, se detallan los resultados:

Tabla 4

Distribución de frecuencias de la dimensión 3

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Muy bajo	105	22,63
Bajo	18	3,88
Medio	197	42,46
Alto	144	31,03
Muy alto	0	0,00
Total	**464**	**100,00**

Nota. Media = 2,82; varianza = 1,22.

La Tabla 4 presenta los resultados del Ítem 5, correspondiente a la dimensión Conocimiento Técnico Operativo. Los hallazgos revelan que el nivel predominante en la muestra fue "Medio", con una frecuencia relativa de 42,46%, seguido por el nivel "Alto" con 31,03%. Un dato de especial relevancia, y que confirma la brecha formativa en la organización, es que un 0% de los colaboradores alcanzó el nivel "Muy Alto", lo que evidencia una ausencia total de *expertise* avanzado en materia de IA. La media obtenida de 2,82 puntos sobre cinco indica que los colaboradores de La Fabril

S.A. presentan un nivel general medio-bajo en esta dimensión. La varianza de 1,22 refleja una dispersión moderada en las percepciones. Este resultado es coherente con los hallazgos de Zhu y Abd Rozan (2026), quienes señalan que la falta de conocimiento técnico operativo es una barrera crítica que impide al personal diferenciar entre el uso de herramientas de IA públicas y versiones corporativas seguras, facilitando prácticas de alto riesgo informático.

4.1.4 Análisis de la Dimensión 4: Percepción de Riesgo de Ciberseguridad

La Dimensión 4 mide la capacidad de los colaboradores para asociar amenazas de vulnerabilidad digital con el uso de la IA. Para ello, se utilizó el ítem: *"¿Qué nivel de riesgo de ciberseguridad y fuga de datos asocia usted al uso de herramientas de IA en el entorno laboral?"*. A continuación, en la Tabla 5, se detallan los resultados:

Tabla 5

Distribución de frecuencias de la dimensión 4

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Muy bajo	95	20,47
Bajo	26	5,60
Medio	118	25,43
Alto	176	37,94
Muy alto	49	10,56
Total	**464**	**100,00**

Nota. Media = 3,12; varianza = 1,66.

La Tabla 5 presenta los resultados del Ítem 2, correspondiente a la dimensión Percepción de Riesgo de Ciberseguridad. Los hallazgos revelan que el nivel predominante en la muestra fue "Alto", con una frecuencia relativa de 37,94%, seguido por el nivel "Medio" con 25,43%. La media obtenida de 3,12 puntos indica que los colaboradores de La Fabril S.A. presentan una percepción del riesgo moderada. La varianza de 1,66 refleja una dispersión también moderada en las percepciones. Este resultado es coherente con lo señalado por Diro et al. (2025), quienes explican que en la era de la IA generativa, una percepción de riesgo moderada-alta es un indicador clave de conciencia situacional. No obstante, esto no garantiza por sí misma la capacidad técnica para mitigar dichas amenazas, lo que introduce la paradoja central de este estudio: los colaboradores perciben el peligro, pero carecen de las herramientas para enfrentarlo.

4.1.5 Análisis de la Dimensión 5: Capacidad para Identificar Vulnerabilidades

La Dimensión 5 mide la habilidad operativa del personal para detectar situaciones que comprometan la seguridad de la información. Para ello, se utilizó el ítem: *"¿Cuál es su nivel de capacidad para identificar cuándo el uso de una IA podría comprometer la privacidad o confidencialidad de la información corporativa?"*. A continuación, en la Tabla 6, se detallan los resultados:

Tabla 6

Distribución de frecuencias de la dimensión 5

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Muy bajo	13	2,80
Bajo	107	23,06
Medio	107	23,06
Alto	189	40,74
Muy alto	48	10,34
Total	**464**	**100,00**

Nota. Media = 3,33; varianza = 1,06.

La Tabla 6 presenta los resultados del Ítem 3, correspondiente a la dimensión Capacidad para Identificar Vulnerabilidades. Los hallazgos revelan que el nivel predominante en la muestra fue "Alto", con una frecuencia relativa de 40,74%. Es interesante notar un empate en el segundo lugar entre los niveles "Bajo" y "Medio", ambos con un 23,06%. La media obtenida de 3,33 puntos indica que los colaboradores de La Fabril S.A. presentan una capacidad moderada para identificar riesgos. La varianza de 1,06 refleja una dispersión relativamente baja, sugiriendo cierto consenso.

Este resultado es coherente con lo señalado por Oyebisi y Orim (2026) sobre la capacidad defensiva práctica; un nivel de percepción medio-alto sugiere que, si bien los colaboradores son conscientes de que existe un riesgo, no poseen las destrezas técnicas especializadas para identificar con total precisión cuándo o cómo una herramienta de IA compromete la seguridad de información de la empresa.

4.1.6 Análisis de la Dimensión 6: Importancia de la Evaluación de Riesgos

La Dimensión 6 mide el grado de valoración que los colaboradores atribuyen a la necesidad de analizar los riesgos antes de implementar una nueva tecnología. Para ello, se utilizó el ítem: *"¿Qué grado de importancia le otorga a la necesidad de evaluar críticamente los riesgos de seguridad y ética antes de implementar cualquier nueva herramienta de IA en La Fabril?"*. A continuación, en la Tabla 7, se detallan los resultados:

Tabla 7

Distribución de frecuencias de la dimensión 6

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Nada importante	1	0,22
Poco importante	91	19,61
Neutral	10	2,16
Importante	165	35,56
Muy importante	197	42,45
Total	**464**	**100,00**

Nota. Media = 4,00; varianza = 1,25.

La Tabla 7 presenta los resultados del Ítem 6, correspondiente a la dimensión Importancia de la Evaluación de Riesgos. Los hallazgos revelan que el nivel predominante en la muestra fue "Muy importante", con una frecuencia relativa de 42,45%, seguido por el nivel "Importante" con 35,56%. La media obtenida

de 4,00 puntos exactos sobre una escala de cinco indica que los colaboradores de La Fabril S.A. le otorgan una importancia alta a la evaluación preventiva de riesgos. La varianza de 1,25 refleja una dispersión moderada-baja en las percepciones, mostrando una clara tendencia y consenso de la plantilla hacia los niveles superiores de valoración. Este resultado es coherente con lo señalado por Alsudais (2026) y su concepto del "deber de prudencia tecnológica"; un nivel de importancia tan elevado refleja una demanda explícita por parte de los colaboradores para que la organización implemente procesos formales de evaluación preventiva, validando la necesidad urgente de un marco de gobernanza institucional.

4.1.7 Análisis de la Dimensión 7: Preocupación por Sesgos Algorítmicos

La Dimensión 7 mide el nivel de inquietud del personal respecto a la posibilidad de que la IA genere errores o decisiones injustas. Para ello, se utilizó el ítem: *"Me preocupa que el uso de IA sin lineamientos corporativos claros pueda generar errores operativos, sesgos o decisiones injustas en los procesos de la empresa"*. A continuación, en la Tabla 8, se detallan los resultados:

Tabla 8

Distribución de frecuencias de la dimensión 7

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Totalmente en desacuerdo	3	0,65
En desacuerdo	93	20,04
Ni de acuerdo ni en desacuerdo	88	18,97
De acuerdo	117	25,22
Totalmente de acuerdo	163	35,12
Total	**464**	**100,00**

Nota. Media = 3,74; varianza = 1,34.

La Tabla 8 presenta los resultados del Ítem 7, correspondiente a la dimensión Preocupación por Sesgos Algorítmicos. Los hallazgos revelan que el nivel predominante en la muestra fue "Totalmente de acuerdo", con una frecuencia relativa de 35,12%, seguido por el nivel "De acuerdo" con 25,22%. La media obtenida de 3,74 puntos indica que, en general, los colaboradores de La Fabril S.A. se muestran de acuerdo con esta preocupación. La varianza de 1,34 refleja una dispersión moderada en las percepciones. Este resultado es coherente con lo señalado por Ishag et al. (2026), quienes argumentan que en la era de la IA, una alta preocupación por los sesgos no es un signo de resistencia al cambio, sino una evidencia de conciencia sobre la falibilidad inherente de los algoritmos y la necesidad de una supervisión humana crítica.

4.1.8 Análisis de la Dimensión 8: Valoración de la Supervisión Humana

La Dimensión 8 mide el nivel de acuerdo del personal sobre la necesidad de validar las decisiones automatizadas. Para ello, se utilizó el ítem: *"¿Con qué frecuencia cree que toda solución automatizada con IA dentro de la empresa debe contar con supervisión o validación humana?"*. A continuación, en la Tabla 9, se detallan los resultados:

Tabla 9

Distribución de frecuencias de la dimensión 8

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Nunca	2	0,43
Rara vez	1	0,22
Ocasionalmente	189	40,73
Frecuentemente	131	28,23
Siempre	141	30,39
Total	**464**	**100,00**

Nota. Media = 3,88; varianza = 0,75.

La Tabla 9 presenta los resultados del Ítem 8, correspondiente a la dimensión Valoración de la Supervisión Humana. Los hallazgos revelan que el nivel predominante en la muestra fue "Ocasionalmente", con una frecuencia relativa de 40,73%, seguido de cerca por "Siempre" con un 30,39%. La media obtenida de 3,88 puntos sobre cinco, cercana a "Frecuentemente", indica un fuerte apoyo de los colaboradores de La Fabril S.A. a la necesidad de supervisión. La varianza de 0,75, una de las más bajas del estudio, refleja un consenso muy robusto en las

percepciones. Este resultado es coherente con los hallazgos de Zhu y Abd Rozan (2026) y su defensa del enfoque "human-in-the-loop"; la alta valoración y el bajo disenso demuestran que el personal no desea delegar ciegamente las decisiones críticas a los algoritmos, sino que busca de forma mayoritaria un modelo de colaboración donde la tecnología actúe como una herramienta de apoyo, pero el juicio final recaiga en el criterio humano.

4.1.9 Análisis de la Dimensión 9: Conciencia del Riesgo Sistémico

La Dimensión 9 evalúa si el personal reconoce que la seguridad informática es una responsabilidad de todos. Para ello, se utilizó el ítem: *"Pienso que adoptar herramientas de IA sin una adecuada gestión de seguridad informática aumenta significativamente la vulnerabilidad de los sistemas de La Fabril"*. A continuación, en la Tabla 10, se detallan los resultados:

Tabla 10

Distribución de frecuencias de la dimensión 9

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Totalmente en desacuerdo	2	0,43
En desacuerdo	2	0,43
Ni de acuerdo ni en desacuerdo	95	20,47
De acuerdo	215	46,34
Totalmente de acuerdo	150	32,33
Total	**464**	**100,00**

Nota. Media = 4,10; varianza = 0,58.

La Tabla 10 presenta los resultados del Ítem 9, correspondiente a la dimensión Conciencia del Riesgo Sistémico. Los hallazgos revelan que el nivel predominante en la muestra fue "De acuerdo", con una frecuencia relativa de 46,34%, seguido por el nivel "Totalmente de acuerdo" con 32,33%. La media obtenida de 4,10 puntos indica que los colaboradores de La Fabril S.A. están fuertemente de acuerdo con que la adopción de IA sin gestión aumenta la vulnerabilidad. La varianza de 0,58, una de las más bajas del estudio, refleja un consenso casi unánime en la plantilla. Este resultado es coherente con los hallazgos de Diro et al. (2025) sobre la responsabilidad compartida; un nivel de acuerdo tan alto y homogéneo demuestra que el personal es consciente de que la seguridad no depende solo del departamento de TI, sino que el comportamiento de cada individuo puede comprometer la red completa, reforzando la necesidad de políticas de gobernanza que involucren a toda la organización.

4.1.10 Análisis de la Dimensión 10: Demanda de Políticas de Gobernanza

La Dimensión 10 evalúa el nivel de apoyo del personal hacia la creación de normativas internas sobre el uso de IA. Para ello, se utilizó el ítem: *"Estoy a favor de que La Fabril establezca, documente y difunda políticas o protocolos explícitos sobre el uso permitido, ético y seguro de la IA"*. A continuación, en la Tabla 11, se detallan los resultados:

Tabla 11

Distribución de frecuencias de la dimensión 10

Categoría	Frecuencia absoluta (f)	Frecuencia relativa (%)
Totalmente en desacuerdo	2	0,43
En desacuerdo	0	0,00
Ni de acuerdo ni en desacuerdo	6	1,29
De acuerdo	149	32,11
Totalmente de acuerdo	307	66,17
Total	**464**	**100,00**

Nota. Media = 4,64; varianza = 0,31.

La Tabla 11 presenta los resultados del Ítem 10, correspondiente a la dimensión Demanda de Políticas de Gobernanza. Los hallazgos son excepcionales y revelan que el nivel predominante en la muestra fue "Totalmente de acuerdo", con una abrumadora frecuencia relativa de 66,17%, seguido por el nivel "De acuerdo" con 32,11%. La media obtenida de 4,64 puntos, cercana al máximo posible, indica que los colaboradores de La Fabril S.A. están casi rotundamente a favor de la creación de políticas. La varianza de 0,31, la más baja de todo el estudio, confirma un consenso casi absoluto en la plantilla. Este resultado es coherente con los hallazgos de Deloitte (2024), donde se constata que la existencia de políticas de TI formales y de carácter ético responde a una necesidad unificada del propio personal, quienes buscan en la normativa corporativa un refugio de seguridad jurídica y operativa que les permita

interactuar con sistemas de IA dentro de un marco de confianza y legalidad institucional.

4.2. Análisis de Confiabilidad

Con el objetivo de determinar la consistencia interna y la estabilidad del instrumento de recolección de datos aplicado a los 464 colaboradores de La Fabril S.A., se realizó el análisis de confiabilidad mediante el coeficiente Alfa de Cronbach. Este análisis estadístico permite evaluar la correlación entre los 10 ítems del cuestionario, garantizando que midan de manera estable las variables del estudio. A continuación, en la Tabla 12, se detallan los resultados de la prueba de confiabilidad:

Tabla 12

Resultados del coeficiente de confiabilidad alfa de Cronbach

Instrumento	Número de Ítems	Alfa de Cronbach	Interpretación
Cuestionario de seguridad y ética en el uso de IA	10	0,933	Excelente

Nota. Los datos procesados a partir de las respuestas de 464 colaboradores en La Fabril S.A.

La Tabla 12 presenta el resultado general del análisis de consistencia interna del instrumento aplicado. Los hallazgos revelan un coeficiente Alfa de Cronbach de 0,933 para el conjunto de los 10 ítems evaluados. De acuerdo con los criterios de clasificación de George y Mallery (2003), un coeficiente superior a 0,90 indica una consistencia interna excelente, lo que demuestra que el instrumento posee una fiabilidad sobresaliente. Este resultado garantiza que el cuestionario está libre de errores de medida significativos y es altamente estable, validando la idoneidad de los datos recolectados para proceder con el análisis inferencial y la prueba de hipótesis.

4.3. Comprobación de Hipótesis

Para dar respuesta al segundo objetivo específico y verificar la hipótesis general de la investigación, se aplicó la prueba no paramétrica de Chi-cuadrado de Pearson (X^2). Este procedimiento estadístico permite evaluar si existe una relación estadísticamente significativa entre la variable independiente (Ítem 5: Conocimiento técnico operativo) y la variable dependiente (Ítem 6: Importancia de la evaluación de riesgos).

El primer paso consistió en la construcción de una tabla de contingencia para visualizar la distribución de las frecuencias observadas en el cruce de ambas variables.

Tabla 13

Tabla de contingencia: Ítem 5 (V.I.) vs. Ítem 6 (V.D.)

Ítem 5 (V.I.) / Ítem 6 (V.D.)	**Nada imp. (1)**	**Poco imp. (2)**	**Neutral (3)**	**Importante (4)**	**Muy imp. (5)**	**Total**
Muy bajo	1	91	2	10	1	105
Bajo	0	0	2	2	14	18
Medio	0	0	4	149	44	197
Alto	0	0	2	4	138	144
Total	**1**	**91**	**10**	**165**	**197**	**464**

Una vez estructurada la tabla de contingencia, se procedió al cálculo de los valores del estadístico no paramétrico Chi-cuadrado de Pearson para evaluar la significancia de la relación. En la Tabla 14, se resumen los resultados obtenidos en la prueba de hipótesis:

Tabla 14

Resultados de la prueba de Chi-cuadrado de Pearson

Estadístico / Parámetro	Valor obtenido
Chi-cuadrado de Pearson $\left(X^2\right)$	640,53
Grados de libertad (gl)	12,00
Valor crítico $X^2(12;\ \alpha\ =\ 0{,}05)$	21,03
p-valor	< 0,001
Decisión estadística	Rechazar H_0 / Aceptar H_1

Nota. Datos calculados con un nivel de confianza del 95% $(\alpha\ = 0{,}05)$ a partir de la muestra de 464 colaboradores.

La Tabla 14 detalla los valores estadísticos resultantes de la prueba inferencial. Los hallazgos revelan que el valor de Chi-cuadrado calculado $(X^2 = 640{,}53)$ supera de manera drástica al valor crítico de la distribución teórica $(X^2 = 21{,}03)$ para 12 grados de libertad. Asimismo, el p-valor obtenido $(p < 0{,}001)$ es estrictamente inferior al nivel de significancia establecido $(\alpha\ = 0{,}05)$. Bajo estos rigurosos parámetros estadísticos, se dispone de evidencia empírica irrefutable para rechazar la Hipótesis Nula (H_0) y aceptar la Hipótesis Alternativa (H_1).

Más allá del formalismo matemático, la extraordinaria magnitud de este estadístico revela una dinámica conductual profunda dentro de La Fabril S.A. Al comprobarse una dependencia tan robusta entre el nivel de conocimiento técnico (V.I.) y la importancia atribuida a la evaluación de riesgos (V.D.), se demuestra que la prudencia tecnológica no surge de manera espontánea en el entorno laboral, sino que es un subproducto directo de la alfabetización digital. En otras palabras, la ignorancia técnica fomenta la subestimación de las amenazas, mientras que la instrucción práctica detona el sentido de responsabilidad y la exigencia de controles. Este hallazgo valida empíricamente la

hipótesis general del estudio y justifica, con plena solidez científica, la urgencia de estructurar el marco de gobernanza corporativa que se propondrá en el Capítulo VI.

4.4. Síntesis e interpretación de Resultados

El análisis descriptivo de las diez dimensiones evaluadas permite diagnosticar con precisión la realidad operativa de La Fabril S.A. frente a la adopción de la Inteligencia Artificial. Los hallazgos revelan un escenario caracterizado por una marcada asimetría entre las competencias reales del personal y su nivel de alerta. Por un lado, la Variable Independiente (D1-D3) expone una profunda brecha formativa: existe una alta polarización en la claridad ética, una exclusión de casi el 22% del personal en temas de capacitación, y un dato crítico que revela que el 0% de la muestra posee un conocimiento técnico "Muy Alto". Esto confirma que la fuerza laboral interactúa con la IA desde la improvisación y sin el *expertise* necesario para salvaguardar la información corporativa.

Por otro lado, y de forma contrastante, la Variable Dependiente (D4-D10) demuestra que esta carencia técnica no se traduce en ignorancia frente al peligro. Los colaboradores exhiben una elevada conciencia situacional: perciben los riesgos de ciberseguridad, temen la aparición de sesgos algorítmicos y reconocen que la vulnerabilidad de la IA es un riesgo sistémico. Esta tensión culmina en el hallazgo más contundente del estudio (Dimensión 10), donde el personal, respaldado por la varianza más baja de toda la investigación $(0{,}31)$, demanda de manera casi unánime la creación de políticas de gobernanza explícitas. El trabajador de La Fabril no rechaza la tecnología, sino que exige un marco normativo que lo proteja de la incertidumbre operativa.

Finalmente, la prueba de hipótesis mediante el estadístico Chi-cuadrado de Pearson $(X^2 = 640{,}53;\ p < 0{,}001)$ da sustento inferencial a esta dinámica, comprobando estadísticamente que el nivel de conocimiento técnico es un factor determinante en la importancia que se le otorga a la evaluación preventiva de riesgos. En suma, los datos empíricos obtenidos en este capítulo justifican de manera irrefutable la necesidad de transitar desde una adopción pasiva e individual de la IA hacia un modelo institucional regulado, cimentando las bases científicas para el diseño del marco de gobernanza y alfabetización digital que se propondrá en la fase culminante de esta investigación.

CAPÍTULO V: Conclusiones, Discusión y Recomendaciones

5.1. Discusión

En relación con el primer objetivo específico, los resultados descriptivos del Capítulo IV revelan que los colaboradores de La Fabril S.A. presentan niveles de claridad ética (D1: media = 2,64), frecuencia de capacitación (D2: media = 3,17) y conocimiento técnico operativo (D3: media = 2,82) que en conjunto configuran una evidente y profunda brecha formativa. El hallazgo más revelador de este diagnóstico es que un absoluto 0% de la muestra alcanzó el nivel "Muy Alto" en D3, confirmando la ausencia total de *expertise* avanzado en materia de IA dentro de la organización.

Este diagnóstico converge con las investigaciones de Mariani et al. (2026), quienes identificaron que la alfabetización algorítmica es sistemáticamente el perfil de competencias menos desarrollado en los entornos laborales actuales, propiciando que el personal interactúe con la tecnología de forma intuitiva. Del mismo modo, el hecho de que un 21,98% de la muestra reporte nunca haber recibido capacitación formal en ética y seguridad digital (D2) materializa la advertencia de Sing et al. (2026): la exclusión de segmentos del personal de los planes de formación se traduce en un detrimento directo de la conciencia operativa frente a las vulnerabilidades.

No obstante, al contrastar estos resultados empíricos con la literatura regional, emerge un hallazgo que aporta un matiz particular al estudio: la alta polarización encontrada en la dimensión de claridad ética (D1), donde contrastan respuestas de nivel "Muy Bajo" (35,78%) con niveles "Altos" (29,09%). A diferencia de los estudios globales que asumen un desconocimiento homogéneo, este fenómeno de asimetría confirma lo documentado en la reciente literatura sobre transformación digital en América Latina. En el contexto corporativo regional, la adopción tecnológica suele darse de manera fragmentada o "en silos"; es decir, mientras algunos colaboradores

avanzan de forma autodidacta generando sus propios criterios de uso, otros quedan completamente rezagados al no existir políticas corporativas estandarizadas, provocando una peligrosa descentralización del conocimiento.

Respecto al segundo objetivo específico, enfocado en evaluar estadísticamente la relación entre las variables, la prueba inferencial arrojó datos reveladores. El cruce entre el conocimiento técnico operativo (D3) y la importancia otorgada a la evaluación de riesgos (D6) generó un estadístico Chi-cuadrado de 640,53 ($p < 0,001$). Esta magnitud resulta excepcional, ya que supera ampliamente los valores críticos encontrados en estudios organizacionales similares, como los analizados por Xiong et al. (2026), quienes reportaron asociaciones mucho más moderadas en empresas de manufactura tradicional. Esta contundencia estadística en la organización confirma los postulados de Alsudais (2026), validando que existe una dependencia directa y proporcional: a mayor instrucción digital, mayor es el nivel de prudencia y exigencia de controles por parte del empleado.

Las implicaciones de esta relación (Variable Independiente influyendo sobre la Variable Dependiente) transforman por completo el enfoque tradicional de la estrategia de capacitación. Los resultados demuestran que la formación tecnológica ya no debe entenderse como un simple entrenamiento operativo para usar un software, sino como el principal mecanismo estratégico para despertar la conciencia situacional. En otras palabras, capacitar al personal es la única vía para que dejen de ser usuarios pasivos y se conviertan en la primera línea de defensa de la ciberseguridad corporativa.

El análisis de las dimensiones de la Variable Dependiente introduce una aparente paradoja que constituye el núcleo de esta investigación. A pesar de la brecha formativa documentada (con medias de 2,64 en D1 y 2,82 en D3), los colaboradores

exhiben niveles sorprendentemente altos de conciencia del riesgo. Dimensiones como la Percepción de Riesgo (D4: media = 3,12), la Preocupación por Sesgos (D7: media = 3,74) y la Conciencia del Riesgo Sistémico (D9: media = 4,10) demuestran que el personal de la organización no es ingenuo frente a las amenazas de la IA.

Este fenómeno de "alta percepción, baja capacidad" no es un hallazgo nuevo, sino que confirma empíricamente lo que Diro et al. (2025) describen como la principal vulnerabilidad de la era de la IA generativa: los empleados son conscientes del peligro porque lo ven en noticias y en su vida diaria, pero carecen de la "capacidad defensiva práctica" que Oyebisi y Orim (2026) definen como indispensable. La situación es un caso de estudio perfecto de esta dinámica: el personal sabe que no debe compartir información sensible, pero no tiene las competencias técnicas para identificar con precisión qué es una herramienta de IA segura o cómo una simple consulta puede filtrar datos confidenciales. Esta paradoja es el principal argumento que justifica la necesidad urgente de un marco de gobernanza, ya que el problema no es la falta de conciencia, sino la falta de herramientas y protocolos para actuar en consecuencia.

El hallazgo más contundente y que redefine el rumbo estratégico de la organización se encuentra en la Dimensión 10 (Demanda de Políticas de Gobernanza). Con una media excepcional de 4,64 puntos y una varianza histórica de apenas 0,31 —que representa el consenso más robusto de toda la investigación—, el 98,28% del personal apoya de forma casi unánime la creación de políticas y protocolos formales de uso de IA en el entorno laboral. Este nivel de acuerdo prácticamente unánime sobrepasa los análisis tradicionales de Deloitte (2024), donde la normativa suele ser vista únicamente como una garantía de seguridad jurídica para la organización. En este caso, los datos revelan que la demanda de regulación no nace de una imposición de la alta gerencia, sino de una exigencia espontánea de la propia fuerza laboral, la

cual se siente expuesta ante la falta de directrices éticas.

Esta movilización de la opinión interna es coherente con el enfoque socio-técnico propuesto por Lucas et al. (2026), el cual postula que el éxito de la transformación digital no depende exclusivamente de la infraestructura de TI, sino de la autorregulación ética de las personas que interactúan con ella. Los colaboradores demuestran que no sufren de tecnofobia o resistencia al cambio; al contrario, quieren usar la IA, pero exigen que la empresa salde su deuda regulatoria para poder innovar dentro de un marco de confianza, legalidad e integridad corporativa.

Finalmente, la comprobación de la Hipótesis General mediante la prueba de Chi-cuadrado ($X^2 = 640{,}53;\ p < 0{,}001$) sirve como el pilar científico que unifica toda la investigación. El resultado demuestra matemáticamente que la brecha de conocimiento (V.I.) y la percepción de riesgo (V.D.) están directamente conectadas. Este hallazgo valida la necesidad de implementar una "gobernanza multicapa" como la que propone Prabha et al. (2026), donde se entiende que las políticas éticas, la capacitación y la seguridad de la información deben funcionar como un sistema integrado y no como departamentos aislados.

En definitiva, el escenario diagnosticado en la empresa expone lo que Mikkilineni y Kelly (2026) llaman una "deuda de coherencia operativa". La adopción de herramientas de IA sin una guía clara ha creado un vacío de control que pone en riesgo la información. Saldar esta deuda requiere, de forma obligatoria, abandonar la improvisación. La fuerza de la hipótesis confirmada en este estudio es clara: el diseño y la implementación de un marco de gobernanza no es una opción de gestión, sino el único camino lógicamente válido para reducir la vulnerabilidad informática que se ha demostrado en este capítulo.

5.2. Conclusiones

El escenario actual de La Fabril S.A. frente al uso de la Inteligencia Artificial muestra una adopción tecnológica rápida, pero carente del acompañamiento institucional necesario, lo cual configura una profunda brecha formativa. Este diagnóstico se confirma al observar los bajos niveles de claridad ética (D1: media = 2,64) y conocimiento técnico operativo (D3: media = 2,82) en el personal. El hallazgo más crítico es que ningún colaborador (0%) alcanzó el nivel "Muy Alto" en el dominio de estas herramientas, evidenciando una falta total de personal especializado. Además, casi una cuarta parte de la plantilla (21,98%) reportó nunca haber recibido capacitación formal (D2: media = 3,17). Esta suma de carencias hace que los trabajadores interactúen con la IA desde la improvisación y la incertidumbre, convirtiendo al usuario sin preparación en la mayor vulnerabilidad informática para la compañía.

Por otro lado, la investigación demuestra que la prudencia al usar la tecnología depende directamente del nivel de alfabetización digital del colaborador. La prueba de hipótesis Chi-cuadrado, que cruzó el conocimiento técnico con la importancia de evaluar riesgos, arrojó un estadístico contundente $(X^2 = 640{,}53; gl = 12; p < 0{,}001)$. Esta magnitud, que supera de forma abrumadora al valor crítico esperado (21,03), brinda la evidencia empírica necesaria para rechazar la Hipótesis Nula. Esto confirma que, a mayor instrucción digital, el empleado exige mayor rigor en los controles preventivos. Por lo tanto, la capacitación en ciberseguridad debe dejar de verse como un simple gasto operativo para convertirse en la estrategia central que transforme a los trabajadores en la primera línea de defensa.

Asimismo, el estudio revela una "paradoja corporativa" que define la situación de la empresa: los colaboradores poseen una alta conciencia del riesgo sistémico (D9:

media = 4,10), pero carecen de las competencias técnicas para mitigarlo. Ante esta realidad de exposición consciente, surge un consenso histórico en la plantilla. Con un acuerdo prácticamente unánime (D10: media = 4,64; varianza = 0,31), el personal exige que la empresa establezca directrices claras para el uso ético y seguro de la IA. En conclusión, esta fuerte demanda de regulación interna responde de manera directa al objetivo general de la investigación, demostrando que el éxito de la transformación digital no depende únicamente de la adquisición de herramientas tecnológicas, sino de saber guiar y proteger al factor humano. Los datos obtenidos en este estudio justifican de manera empírica e irrefutable la necesidad de diseñar e implementar un Marco de Gobernanza —propuesto en el Capítulo VI de este trabajo— que dote a la organización de políticas definidas, normas de protección de datos y un programa de formación continuo que cierre definitivamente la brecha diagnosticada.

5.3. Recomendaciones y Limitaciones

Recomendaciones

En primer lugar, se recomienda a la Gerencia General, al área de Tecnología de la Información y a Talento Humano de La Fabril S.A. implementar, de manera inmediata en un plazo no mayor a seis meses, el programa de capacitación en ética digital propuesto en el Capítulo VI de este estudio. Esta iniciativa formativa debe priorizar de manera urgente al segmento de la plantilla que reportó nunca haber recibido instrucción en la materia (21,98%), diseñando paralelamente políticas institucionales claras sobre el uso aceptable de herramientas de Inteligencia Artificial para eliminar el actual vacío de control.

En segundo lugar, se aconseja a la Dirección de TI de la empresa conformar, a corto plazo y en un horizonte de seis a doce meses, un Comité de Gobernanza de IA. Este equipo tendrá la responsabilidad de supervisar el uso diario de las tecnologías

generativas dentro de la organización, definir lineamientos específicos para la clasificación y protección de los datos corporativos, y realizar auditorías de cumplimiento trimestrales que aseguren que la innovación tecnológica no comprometa la seguridad de la compañía.

En tercer lugar, de cara a la comunidad académica, se sugiere replicar a mediano plazo el cuestionario validado en esta investigación en otras empresas del sector manufacturero del país. Esta práctica permitirá realizar estudios comparativos sobre los niveles de preparación digital y percepción del riesgo, contribuyendo a la creación de un indicador regional que mida la madurez de la ética digital en el ámbito corporativo.

Finalmente, en el ámbito de la política pública, se recomienda al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y a las instituciones educativas del Estado incorporar la formación en ética de la IA como un requisito obligatorio en sus programas de capacitación técnica a mediano plazo. Esta acción estratégica permitirá alinear el desarrollo de la fuerza laboral ecuatoriana con los objetivos trazados en la Estrategia Nacional de Inteligencia Artificial 2025–2029.

Limitaciones del estudio

No obstante, la solidez de los hallazgos, el presente estudio tiene limitaciones que deben ser consideradas al momento de interpretar sus resultados, las cuales definen su alcance real con total honestidad académica. En primer lugar, este es un estudio de caso único, lo que significa que los hallazgos se aplican exclusivamente a los colaboradores de La Fabril S.A. y no pueden generalizarse de forma automática a otras empresas del sector manufacturero ecuatoriano sin hacer una investigación comparativa previa. En segundo lugar, la información se obtuvo mediante un cuestionario auto-reportado, lo que introduce la posibilidad de que exista cierta

inclinación en los participantes a responder lo que consideran socialmente "correcto" o esperado, especialmente en los ítems que miden su preocupación por el riesgo de la tecnología o la exigencia de políticas claras. En tercer lugar, debido a que el diseño de la investigación no es experimental, la relación estadística comprobada con la prueba Chi-cuadrado demuestra que una variable depende de la otra, pero no permite establecer de forma matemática una relación directa de causa y efecto. Lejos de restar valor a la tesis, estas limitaciones ayudan a definir con precisión su alcance y abren el camino para futuras investigaciones que busquen aplicar este cuestionario en muestras de diferentes sectores industriales, o realizar de manera longitudinal un seguimiento que evalúe el impacto real de los programas de capacitación sobre la reducción de incidentes de ciberseguridad en las organizaciones.

En respuesta directa a las conclusiones y recomendaciones de este estudio, se ha diseñado el Marco de Gobernanza de Inteligencia Artificial para La Fabril S.A. (MGAI-LF v1.0). Este documento, que constituye el aporte práctico y la solución definitiva a la problemática diagnosticada, se presenta de forma íntegra en el Anexo B de esta investigación.

REFERENCIAS BIBLIOGRÁFICAS

Alsudais, M. (2026). EVOLVING CORPORATE FIDUCIARY DUTIES AND LIABILITIES IN THE ERA OF ARTIFICIAL INTELLIGENCE-DRIVEN SUSTAINABILITY. *Corporate Governance and Sustainability Review*, *10*(3), 110-140. Scopus. https://doi.org/10.22495/cgsrv10i3p9

Arroyo, V. R., Castaño Sánchez, R., & Rocha, A. O. (2026). Transformational impact of technological integration on corporate sustainability: Artificial intelligence adoption from management and employees' perspective. *International Entrepreneurship and Management Journal*, *22*(2). Scopus. https://doi.org/10.1007/s11365-026-01203-y

Ayoub, A. (2026). The Architecture of Intelligent Governance (AIG): A Conceptual Framework for Integration AI, Quantum Computing, and Global Resource Resilience. *Sustainability (Switzerland)*, *18*(5). Scopus. https://doi.org/10.3390/su18052312

Chee, H., Ahn, S., & Lee, J. (2024). A Competency Framework for AI Literacy: Variations by Different Learner Groups and an Implied Learning Pathway. *British Journal of Educational Technology*, *56*, 2146-2182. https://doi.org/10.1111/bjet.13556

Chen, Q., & He, Q. (2026). Research on the Evaluation and Development Strategies of Digital Literacy of Business Teachers under the Background of AI. *ICBDE - Int. Conf. Big Data Educ.*, 91-97. Scopus. https://doi.org/10.1145/3786183.3786185

Cochran, W. G. (1977). *Sampling Techniques* (3.ª ed.). John Wiley & Sons. https://books.google.com.ec/books?id=xbNn41DUrNwC

Coovadia, H., Marx, B., Botha, I., & Gold, N. O. (2025). Building an ethical artificial intelligence corporate governance framework for the integration of emerging technologies into business processes. *South African Journal of Accounting Research*, *39*(3), 286-316. Scopus. https://doi.org/10.1080/10291954.2025.2523661

Deloitte. (2024). *Generating trust in GenAI through training, transparency*. Deloitte Insights. https://action.deloitte.com/insight/4211/generating-trust-in-genai-through-training-

transparency

Deloitte. (2026). *Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en Ecuador (2025-2029)*. https://www.deloitte.com/latam/es/services/legal/perspectives/ec-ecuador-avanza-hacia-el-uso-seguro-etico-y-responsable-de-la-ia.html

Diro, A., Kaisar, S., Saini, A., Fatima, S., Hiep, P. C., & Erba, F. (2025). Workplace security and privacy implications in the GenAI age: A survey. *Journal of Information Security and Applications*, *89*. Scopus. https://doi.org/10.1016/j.jisa.2024.103960

European Parliament and Council of the European Union. (2024). *Artificial Intelligence Act (EU AI Act)—Regulation (EU) 2024/1689*. Unión Europea. http://data.europa.eu/eli/reg/2024/1689/oj

Fineberg, S., Hupfer, S., Loucks, J., Steinhart, M., & Mazumder, S. (2025). *In the gen AI economy, consumers want innovation they can trust*. Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html

Galarza-Sánchez, P. C., Boné-Andrade, M. F., & Pinargote-Bravo, V. J. (2023). Aplicaciones de inteligencia artificial generativa en la transformación digital empresarial. *Revista Científica Ciencia y Método*, *1*(1), 28-41. https://doi.org/10.55813/gaea/rcym/v1/n1/8

George, D., & Mallery, P. (2003). *SPSS for Windows Step by Step: A Simple Guide and Reference*. Allyn & Bacon.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

IBM Security. (2025). *Coste de una filtración de datos en 2025 | IBM*. https://www.ibm.com/reports/data-breach

ISACA. (2019). *COBIT 2019 Framework Governance and Management Objectives*. ISACA.

Ishag, K. I. A., Setoutah, S., Mahmoud, K. O., Al-Obaidi, E., & Mohamed, E. A. S. (2026). The Impact of Generative Artificial Intelligence on Public Relations Strategies: A Shift

in Practitioner Roles and the Future of Corporate Communication. *Studies in Media and Communication*, *14*(3), 250-257. Scopus. https://doi.org/10.11114/smc.v14i3.8719

Lucas, S., Heinitz, R. M., Becker, S. J., & Charton, J. E. (2026). Developing a framework for addressing ethical challenges in generative AI. *Journal of Information Technology Case and Application Research*, *28*(1), 15-29. Scopus. https://doi.org/10.1080/15228053.2025.2558443

Mariani, C., Mancini, M., & Aaltonen, K. (2026). Mind the gap: Project managers, AI literacy, and the future of project management competences. *Project Leadership and Society*, *7*. Scopus. https://doi.org/10.1016/j.plas.2026.100219

Mazzinghy, A. O. da C., Silva, R. M. dos S. e, Fernandes, R. M., Batista, E. D., Picanço, A. R. S., Monteiro, N. J., de Amorim, D. M., Cardoso, B. de F. O., Silva, J. M. N. da, & Martins, V. W. B. (2025). Assessment of the Benefits of the ISO/IEC 42001 AI Management System: Insights from Selected Brazilian Logistics Experts: An Empirical Study. *Standards*, *5*(2), 10. https://doi.org/10.3390/standards5020010

Méndez, S. F., & Aquilina Fueyo Gutiérrez, M. (2025). Accelerationism, AI Safety, and Education: Technocapitalist Discourses on AI Alignment and their Educational Implications. *Revista Espanola de Educacion Comparada*, *48*, 354-379. Scopus. https://doi.org/10.5944/reec.48.2025.45369

Mikkilineni, R., & Kelly, W. P. (2026). The Missing Layer in Modern IT: Governance of Commitments, Not Just Compute and Data. *Computers*, *15*(5). Scopus. https://doi.org/10.3390/computers15050275

MINTEL. (2026). *Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en el Ecuador (EFIA-EC)* (Acuerdo Ministerial Nro. MINTEL-MINTEL-2025-0030, Registro Oficial Primer Suplemento No. 206). Ministerio de Telecomunicaciones y de la Sociedad de la Información. https://strapi.lexis.com.ec/uploads/Registro_Oficial_Ano_I_Primer_Suplemento_No_2

06_del_19_de_enero_de_2026_LEXIS_ECUADOR_86fc2da374.pdf

Moreira Mera, E. (2025, julio 3). *Ciberdelincuencia avanza en Ecuador y la justicia no logra alcanzarla: ¿Hay solución?* Diario Expreso. https://www.expreso.ec/actualidad/ciberdelincuencia-avanza-ecuador-justicia-no-logra-alcanzarla-solucion-248549.html

NIST. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1; p. NIST AI 100-1). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.AI.100-1

Oyebisi, D., & Orim, S.-M. (2026). Securing responsible AI: Integrating cybersecurity and AI governance at NovexTech solutions. *Journal of Information Technology Teaching Cases*. Scopus. https://doi.org/10.1177/20438869261448219

Podevin, D., Paulus, M., Wilhelm, A., & Hellbrück, N. (2026). Responsible Marketing in the Age of AI: Ethical Reflection for Companies Between Innovation and Responsibility. *Commun. Comput. Info. Sci.*, *2666 CCIS*, 216-228. https://doi.org/10.1007/978-3-032-08614-3_13

Prabha, K. R., Mabel, B. R., Isaev, F., Mamadiyarov, Z., Raxmatullayevich, K. U., Erkinjon, T., & Khurramova, M. (2026). A Multi-Layer Artificial Intelligence– Enabled Governance Framework for Integrating Information Security Management, Quality Management, and Strategic Human Resource Analytics: An Empirical Study on the Role of Corporate Social Responsibility in Sustainable Organizational Performance. *Quality - Access to Success*, *27*(210), 418-426. Scopus. https://doi.org/10.47750/QAS/27.210.45

Ray, S. (2023). 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/

Scherz, P. (2025). Automation and Augmentation in Theological Perspective. *Modern Theology*. Scopus. https://doi.org/10.1111/moth.70063

Sing, R. D. R., Hassan, N. H. S. B., Shaqman, N., & Kumar, P. (2026). Unveiling the Impact of AI Utilization, Tools, and Training on Work Efficiency: A Mediation Analysis of Task Typologies. *Indian Journal of Information Sources and Services*, *16*(2), 556-567. Scopus. https://doi.org/10.51983/ijiss-2026.16.2.56

Sistema Económico Latinoamericano y del Caribe (SELA). (2025). *Gobernanza Ética de la Inteligencia Artificial: Grandes Empresas Tecnológicas, Inteligencia Artificial y la Gobernanza Global Tecnológica*. Secretaría Permanente del SELA. https://sela.org/publicaciones/gobernanza-etica-de-la-inteligencia-artificial-grandes-empresas-tecnologicas-inteligencia-artificial-y-la-gobernanza-global-tecnologica/

Telégrafo, E. (2025, abril 17). *Inteligencia Artificial: El 40% de las empresas en Ecuador ya la implementó*. El Telégrafo. https://www.eltelegrafo.com.ec/noticias/tendencias/190/inteligencia-artificial-el-40-de-las-empresas-en-ecuador-ya-la-implemento

Torres Gamarra, N., & Zúñiga Carnero, M. (2025). *Panorama actual de la ciberseguridad: Amenazas, legislación y brechas estructurales desde una revisión sistemática*. https://doi.org/10.5281/zenodo.15605545

Xiong, M., Xu, H., Ji, J., Zuo, R., Wang, Y., & Olya, H. (2026). Responsible Artificial Intelligence Attention and Firm Innovation: An Attention-Based View. *Journal of Product Innovation Management*, *43*(1), 186-214. Scopus. https://doi.org/10.1111/jpim.70015

Zhu, T., & Abd Rozan, M. Z. (2026). AI adoption in E-commerce enterprises: Insights into current practices and future directions from an interview study. *PLOS ONE*, *21*(3 March). Scopus. https://doi.org/10.1371/journal.pone.0336416

ANEXOS

Anexo A

Cuestionario de Percepción sobre Seguridad y Ética en el uso de IA

Objetivo: Analizar la percepción de los colaboradores de La Fabril S.A. sobre los aspectos éticos, los riesgos de seguridad y el nivel de preparación frente al uso de la Inteligencia Artificial en sus procesos de transformación digital.

A continuación, se presentan algunas afirmaciones. Indique el grado en que está de acuerdo con cada una.

Parte I: Datos de Perfil (Demográficos)

Edad (Seleccione el rango al que pertenece)

( ) 18 - 25 años

( ) 26 - 35 años

( ) 36 - 45 años

( ) 46 - 55 años

( ) Más de 55 años

Área o Departamento en La Fabril *¿En qué área principal de la empresa desempeña sus funciones?*

( ) Tecnología de la Información (TI) / Sistemas

( ) Administración y Finanzas

( ) Recursos Humanos / Talento Humano

( ) Comercial / Ventas / Marketing

( ) Operaciones / Producción / Logística (Personal administrativo)

( ) Auditoría / Legal / Compliance

( ) Otro:

Nivel Jerárquico o Rol ***¿Cuál es su nivel de responsabilidad actual en la empresa?***

( ) Gerencia / Dirección

( ) Jefatura / Coordinación / Supervisión

( ) Especialista / Analista / Ingeniero

( ) Asistente / Auxiliar administrativo

Antigüedad laboral en La Fabril S.A. ***Seleccione el tiempo que lleva laborando continuadamente en la empresa)***

( ) Menos de 1 año

( ) De 1 a 3 años

( ) De 4 a 6 años

( ) Más de 7 años

Uso actual de Inteligencia Artificial ***¿Utiliza actualmente alguna herramienta de Inteligencia Artificial (ej. ChatGPT, Copilot, Gemini, etc.) para facilitar sus tareas laborales?***

( ) Sí, frecuentemente

( ) Sí, de manera ocasional

( ) No, no utilizo ninguna

Parte II: Preguntas del Instrumento (Ítems 1 al 10)

1. ¿Cuál es su nivel de claridad sobre los principios éticos básicos que deben guiar el uso de herramientas de Inteligencia Artificial en sus funciones dentro de la empresa?

( ) 1 = Muy Bajo

( ) 2 = Bajo

( ) 3 = Medio

( ) 4 = Alto

( ) 5 = Muy Alto

2. ¿Qué nivel de riesgo de ciberseguridad y fuga de datos asocia usted al uso de herramientas de Inteligencia Artificial en el entorno laboral?

( ) 1 = Muy Bajo

( ) 2 = Bajo

( ) 3 = Medio

( ) 4 = Alto

( ) 5 = Muy Alto

3. ¿Cuál es su nivel de capacidad para identificar cuándo el uso de una IA podría comprometer la privacidad o confidencialidad de la información corporativa?

( ) 1 = Muy Bajo

( ) 2 = Bajo

( ) 3 = Medio

( ) 4 = Alto

( ) 5 = Muy Alto

4. ¿En su formación profesional o interna, ¿con qué frecuencia ha recibido capacitación sobre ética y seguridad digital para utilizar la IA de forma responsable?

( ) 1 = Nunca

( ) 2 = Rara vez

( ) 3 = Ocasionalmente

( ) 4 = Frecuentemente

( ) 5 = Muy frecuentemente

5. ¿Cuál es su nivel de conocimiento exacto sobre las medidas de precaución que debe aplicar al utilizar IA en sus procesos diarios de transformación digital?

( ) 1 = Muy Bajo

( ) 2 = Bajo

( ) 3 = Medio

( ) 4 = Alto

( ) 5 = Muy Alto

6. ¿Qué grado de importancia le otorga a la necesidad de evaluar de manera crítica los riesgos de seguridad y ética antes de implementar cualquier nueva herramienta de IA en La Fabril?

( ) 1 = Nada importante

( ) 2 = Poco Importante

( ) 3 = Neutral

( ) 4 = Importante

( ) 5 = Muy Importante

7. "Me preocupa que el uso de IA sin lineamientos corporativos claros pueda generar errores operativos, sesgos o decisiones injustas en los procesos de la empresa."

( ) 1 = Totalmente en desacuerdo

( ) 2 = En desacuerdo

( ) 3 = Ni de acuerdo ni en desacuerdo

( ) 4 = De acuerdo

( ) 5 = Totalmente de acuerdo

8. ¿Con qué frecuencia cree que toda solución automatizada con Inteligencia Artificial dentro de la empresa debe contar con supervisión o validación humana?

( ) 1 = Nunca

( ) 2 = Rara vez

( ) 3 = Ocasionalmente

( ) 4 = Frecuentemente

( ) 5 = Siempre

9. "Pienso que adoptar herramientas de IA sin una adecuada gestión de seguridad informática aumenta significativamente la vulnerabilidad de los sistemas de La Fabril."

( ) 1 = Totalmente en desacuerdo

( ) 2 = En desacuerdo

( ) 3 = Ni de acuerdo ni en desacuerdo

( ) 4 = De acuerdo

( ) 5 = Totalmente de acuerdo

10. "Estoy a favor de que La Fabril establezca, documente y difunda políticas o protocolos explícitos sobre el uso permitido, ético y seguro de la Inteligencia Artificial."

( ) 1 = Totalmente en desacuerdo

( ) 2 = En desacuerdo

( ) 3 = Ni de acuerdo ni en desacuerdo

( ) 4 = De acuerdo

( ) 5 = Totalmente de acuerdo

Anexo B

Propuesta Marco de Gobernanza de Inteligencia Artificial para La Fabril S.A. (MGAI-LF v1.0)

Presentación e introducción de la propuesta

El diagnóstico empírico realizado en el Capítulo IV de esta investigación reveló que los colaboradores de La Fabril S.A. interactúan con herramientas de Inteligencia Artificial desde una posición de vulnerabilidad formativa significativa. En concreto, un 0% de la muestra $(n = 464)$ alcanzó un nivel de *expertise* técnico avanzado en la materia (D3), mientras que casi una cuarta parte del personal (21,98%) reportó nunca haber recibido capacitación formal en ética y seguridad digital (D2). Asimismo, la prueba Chi-cuadrado de Pearson confirmó de manera concluyente que esta brecha de conocimiento determina directamente la capacidad del personal para valorar y mitigar los riesgos operativos $(\chi^2 = 640{,}53;\ gl = 12;\ p < 0{,}001)$. Sorprendentemente, frente a esta carencia técnica, el 98,28% de la plantilla apoya de forma casi total la creación de políticas formales de uso de IA (D10: media = 4,64; varianza = 0,31). Este gran contraste convierte a la presente propuesta en la respuesta directa a una demanda colectiva documentada científicamente.

En respuesta a estos hallazgos, y con el propósito de dar estricto cumplimiento al tercer objetivo específico de la investigación, se propone el presente Marco de Gobernanza de Inteligencia Artificial para La Fabril S.A. (MGAI-LF v1.0). Este es un instrumento institucional que tiene como objetivo central establecer las políticas de uso aceptable, los lineamientos de protección y los programas formativos modulares necesarios para garantizar que la adopción de herramientas algorítmicas en el Complejo Industrial de Montecristi sea un proceso ético, seguro y trazable. Además,

el diseño integral de este marco se encuentra estratégicamente alineado con las directrices de la Estrategia Nacional de Inteligencia Artificial del Ecuador (MINTEL, 2026), asegurando que sea una propuesta útil, legal y viable para la empresa.

Objetivos de la propuesta

Para garantizar la correcta ejecución del MGAI-LF v1.0, se establecen los siguientes objetivos:

Objetivo general

Diseñar un ecosistema integrado de gobernanza de Inteligencia Artificial para La Fabril S.A. que articule políticas de uso permitido, lineamientos de protección de datos y un plan continuo de alfabetización digital para mitigar los riesgos operativos identificados.

Objetivos específicos

Establecer políticas claras de uso aceptable que definan qué herramientas de IA están autorizadas o prohibidas para el personal de la empresa, eliminando la incertidumbre operativa.

1. Diseñar directrices de clasificación de datos institucionales mediante un sistema visual de seguridad, asegurando que la información confidencial de la compañía no sea expuesta en plataformas externas.
2. Estructurar un programa de capacitación modular en seguridad y ética de la IA, orientado a cerrar la brecha formativa del personal y priorizar a los colaboradores sin instrucción previa.

Alcance de la propuesta

El alcance de aplicación del Marco de Gobernanza de Inteligencia Artificial para La Fabril S.A. (MGAI-LF v1.0) se delimita bajo los siguientes criterios organizacionales:

- Alcance Humano: El marco y sus directrices son de aplicación obligatoria para todo el personal de la empresa, abarcando a colaboradores de nivel directivo,

mandos medios, personal administrativo y operativo en todas las sucursales, con especial énfasis en el Complejo Industrial de Montecristi.

- Alcance Tecnológico: La directriz regula el uso de cualquier herramienta, plataforma o sistema basado en Inteligencia Artificial (tanto generativa como predictiva) que sea utilizado para realizar funciones laborales, abarcando desde las herramientas corporativas aprobadas oficialmente por el área de TI hasta las aplicaciones de uso público de libre acceso.
- Alcance Operativo: Las normas del marco rigen sobre toda la información, datos e interacciones que el personal de la compañía procese o ingrese en sistemas de IA durante el desempeño de sus actividades profesionales, asegurando la trazabilidad y la seguridad integral de los activos de información de la firma.

Fundamentación teórica y normativa

El MGAI-LF v1.0 no opera en un vacío regulatorio, sino que se fundamenta en una sólida base legal y en la adopción de los principales marcos de referencia internacionales. En el plano legal, el marco se apoya en el reciente Acuerdo Ministerial Nro. MINTEL-MINTEL-2025-0030, el cual obliga a las organizaciones ecuatorianas a revisar y adaptar sus políticas internas frente a las tecnologías disruptivas (MINTEL, 2026). Asimismo, se alinea con las estrictas exigencias de la Ley Orgánica de Protección de Datos Personales (LOPDP) para proteger la información de colaboradores y clientes, tomando como máximo referente global el enfoque basado en riesgos del Reglamento de Inteligencia Artificial de la Unión Europea (2024).

Desde la perspectiva técnica y procedimental, la propuesta se estructura sobre tres pilares normativos complementarios. En primer lugar, el NIST AI Risk Management

Framework (2023) provee la metodología esencial para identificar y controlar los riesgos algorítmicos a través de sus cuatro funciones centrales: *Mapear, Medir, Gestionar y Gobernar*, dotando de lógica a las políticas de uso. En segundo lugar, COBIT 2019 (ISACA, 2019) asegura el alineamiento estratégico de este marco con los objetivos de negocio de La Fabril S.A., garantizando que la gobernanza de IA no opere como un "silo" aislado del departamento de TI, sino como una función integrada en todo el gobierno corporativo. Finalmente, la norma ISO/IEC 42001:2023 proporciona el estándar formal de gestión que dota al modelo de mecanismos para realizar auditorías y mantener una mejora continua.

En conjunto, la integración de estos componentes legales y técnicos permite materializar y operativizar el enfoque de "gobernanza multicapa" propuesto por Prabha et al. (2026), el cual fue adoptado como la base metodológica central a lo largo de esta investigación.

Componente 1: Políticas de uso aceptable de inteligencia artificial

Este primer componente normativo responde directamente a las vulnerabilidades identificadas en el diagnóstico (Dimensiones D1, D2 y D3), en el cual se evidenció que los colaboradores carecen de directrices claras sobre los límites de uso de la Inteligencia Artificial. Con el objetivo de eliminar esta incertidumbre operativa, se establecen las siguientes reglas esenciales de cumplimiento obligatorio para todo el personal de La Fabril S.A.

Reglas esenciales de la política

1. Uso exclusivo de herramientas autorizadas: El colaborador debe utilizar únicamente las herramientas de IA aprobadas formalmente por el Departamento de Tecnologías de la Información (TI) de La Fabril S.A. y que se encuentren listadas en la matriz de autorización de esta directriz.

2. Prohibición de cargar información confidencial en IA pública: Está estrictamente prohibido ingresar información clasificada como Confidencial o Restringida (tales como recetas industriales, fórmulas de costos, bases de datos de clientes y proyecciones financieras) en herramientas de IA de uso público o personal.
3. Supervisión humana obligatoria: Toda decisión operativa, técnica o estratégica asistida por IA debe ser revisada y validada por un profesional humano antes de su implementación. Ningún proceso crítico corporativo puede ser automatizado sin un punto de control humano explícito.
4. Reporte de incidentes: El colaborador debe reportar al Departamento de TI, dentro de un plazo máximo de 24 horas siguientes a su detección, cualquier situación, falla o comportamiento anómalo que pueda comprometer la seguridad de la información al usar herramientas de IA.
5. Actualización de contraseñas y accesos: Las credenciales de acceso a las herramientas de IA corporativas deben actualizarse obligatoriamente cada 90 días. Está prohibido compartir credenciales, cuentas o perfiles de acceso entre colaboradores o terceros.
6. Participación obligatoria en capacitación: Todo colaborador debe completar el Módulo 1 del programa interno de capacitación en ética digital dentro de los primeros 30 días calendario a partir de la publicación oficial de esta política.

Matriz de clasificación de herramientas de IA

Para garantizar la aplicabilidad inmediata de la Regla 1, a continuación, en la Tabla 15, se detalla el listado de herramientas tecnológicas autorizadas para uso corporativo, contrastándolas con aquellas cuyo uso en el entorno laboral representa un alto riesgo de ciberseguridad.

Tabla 15

Clasificación corporativa de herramientas de IA autorizadas y prohibidas en La Fabril S.A.

Categoría tecnológica	Herramientas autorizadas	Herramientas prohibidas (sin autorización)
IA generativa	Gemini for Workspace (versión corporativa de La Fabril S.A.).	ChatGPT (versión gratuita), Claude.ai (personal), Copilot sin cuenta corporativa.
Procesamiento de documentos	Suite Microsoft 365 corporativa com funciones de IA habilitadas por TI.	Subir documentos internos a plataformas públicas de resumen o traducción (ej. Smallpdf o DeepL con datos sensibles).
Análisis de datos	Excel corporativo, Power BI con acceso institucional, Julius AI con datos previamente anonimizados.	Subir bases de datos de colaboradores, nómina, costos o producción a herramientas de análisis de terceros sin cifrado.
Comunicación	Correo corporativo, Microsoft Teams, y canales internos aprobados por TI.	Enviar información confidencial mediante IA de transcripción o resumen de terceros (ej. Otter.ai, Fireflies) sin contrato previo de confidencialidad.

Nota. El catálogo de herramientas autorizadas será revisado y actualizado semestralmente por el Comité de Gobernanza de IA del Departamento de TI.

Componente 2: Lineamientos de clasificación y protección de datos

Este componente responde directamente a los vacíos identificados en el diagnóstico empírico (Dimensiones D3 y D5), donde se evidenció que los colaboradores carecen de la capacidad técnica para distinguir qué información es segura para ser procesada con herramientas de IA. Para solucionar esta vulnerabilidad, se establece un esquema de clasificación de datos claro, acompañado de responsables directos por cada nivel, detallado a continuación en la Tabla 16.

Tabla 16

Matriz de clasificación de la información y restricciones de uso con IA

Nivel	Tipos de información	Restricción de uso con IA	Responsable
Confidencial (rojo)	Recetas de producción, fórmulas de costos, proyecciones financieras, datos personales de colaboradores.	Está prohibido procesar en cualquier IA pública o no corporativa. Solo permitido en sistemas aprobados por TI con cifrado de extremo a extremo.	Responsable de TI y gerente del área
Restringido (naranja)	Contratos con proveedores, datos de clientes, métricas de producción, KPI's estratégicos.	Procesable solo en Gemini Workspace corporativo. Requiere autorización explícita del jefe directo para uso externo.	Jefe de área y responsable de TI
Interno (amarillo)	Procedimientos operativos, manuales de proceso, correos internos no sensibles.	Procesable en herramientas corporativas autorizadas. No se debe subir a plataformas de uso público sin revisión previa.	Colaborador y jefe directo
Público (verde)	Información ya publicada, comunicados de prensa, datos de catálogos oficiales.	Puede usarse libremente en cualquier herramienta de IA, incluyendo aquellas de uso personal.	Colaborador

Nota. Ante cualquier duda de clasificación, el colaborador debe tratar el documento bajo el nivel de mayor restricción hasta consultar con su superior.

Protocolo de respuesta ante incidentes de seguridad

A pesar de los controles preventivos, es imperativo establecer un plan de contingencia ante posibles brechas. En caso de detectar que información Confidencial o Restringida ha sido expuesta indebidamente en una plataforma de IA, el personal involucrado y el departamento de tecnología deben ejecutar obligatoriamente los pasos descritos en la Tabla 17.

Tabla 17

Protocolo de actuación y respuesta ante incidentes de fuga de datos en IA

Paso	Acción	Detalle operativo
1. Contención	Aislar el sistema o herramienta involucrada.	El colaborador debe cesar inmediatamente el uso de la herramienta de IA y desconectar el equipo de la red si el incidente implica datos confidenciales. No debe borrar ningún archivo.
2. Notificación	Reportar al responsable de TI en máximo 2 horas.	Debe completar el Formulario de Incidente de Seguridad (FIS-001) en la intranet corporativa, indicando: herramienta utilizada, tipo de datos expuestos y acciones previas.
3. Evaluación	TI evalúa el alcance en máximo 24 horas.	El Departamento de TI determina el nivel de exposición, identifica los datos comprometidos y activa el protocolo de comunicación a las áreas afectadas y a la Gerencia General.
4. Remediación y reporte	Acciones correctivas y documentación.	Implementar medidas de mitigación, revocar accesos comprometidos y emitir un informe de incidente al Comité de Gobernanza en un plazo no mayor a 5 días hábiles.

Nota. El incumplimiento de este protocolo de notificación por parte del colaborador será considerado una falta grave a las políticas de seguridad de La Fabril S.A.

Componente 3: Programa Modular de Capacitación en Ética Digital

El tercer componente del marco tiene como objetivo erradicar la brecha formativa diagnosticada en la organización, específicamente la alarmante ausencia de *expertise* avanzado (0% en D3) y la vulnerabilidad del 21,98% del personal que reportó exclusión formativa (D2). Para transformar al colaborador desde un usuario en riesgo hacia un agente activo de defensa, se establece la obligatoriedad del "Programa Modular de Capacitación en Ética Digital y Seguridad IA". Este programa se estructura en tres niveles secuenciales de conocimiento, diseñados para abarcar

desde la alfabetización básica hasta la aplicación técnica segura, tal como se detalla en la Tabla 18.

Tabla 18

Estructura del programa modular de capacitación en IA para La Fabril S.A.

Módulo	Nombre del módulo	Duración	Dirigido a	Contenidos clave	Metodología y evaluación
Módulo 1	Fundamentos de Ética y Seguridad en el uso de IA	4 horas	Todo el personal (464 colaboradores). Obligatorio.	Conceptos de IA ética, *Shadow AI* y sus riesgos, casos reales (Samsung), clasificación básica de información, uso responsable de Gemini corporativo.	Capacitación presencial + material digital. Evaluación: cuestionario de 10 preguntas (nota mínima: 70%).
Módulo 2	Identificación de Vulnerabilidades y Ciberseguridad Operativa	6 horas	Personal con acceso a datos confidenciales y restringidos.	Vectores de ataque por IA generativa, *phishing* e ingeniería social, ejercicios prácticos de clasificación de información, protocolo de reporte de incidentes.	Taller práctico con simulaciones. Evaluación: resolución de casos (aprobación por competencia).
Módulo 3	Gobernanza de IA para Líderes y Tomadores de Decisiones	3 horas	Gerentes, jefes de área y responsables de TI.	ISO/IEC 42001:2023, NIST AI RMF, deber de prudencia tecnológica, diseño e implementación de políticas internas, supervisión del Comité de Gobernanza.	Seminario ejecutivo. Evaluación: diseño de un plan de acción para su área (entregable).

Nota. El Departamento de Talento Humano, en coordinación con la Dirección de TI, es el responsable de ejecutar este programa, asegurar su actualización anual y monitorear el cumplimiento de los colaboradores.

Módulo 1: Fundamentos de Ética y Seguridad en el uso de IA

- Justificación empírica: El diagnóstico reveló que el 35,78% de la muestra presenta un nivel "Muy Bajo" de claridad ética (D1: media = 2,64) y que el 21,98% nunca ha recibido formación en ética digital (D2). Este módulo está diseñado para atacar directamente esta brecha fundamental.
- Objetivo y duración: Al finalizar este módulo de 4 horas, el 100% de los colaboradores de La Fabril S.A. será capaz de comprender los principios básicos del uso ético de la IA, diferenciar entre una herramienta pública y una corporativa, e identificar los riesgos de seguridad más comunes.
- Contenidos: Los temas clave incluyen: (a) conceptos fundamentales de IA; (b) el fenómeno del *Shadow AI* y sus riesgos; (c) casos de estudio de fugas de información (ej. Samsung); y (d) la revisión detallada del Semáforo de Datos Corporativos de la empresa.
- Metodología y evaluación: Este módulo se impartirá en modalidad asincrónica (E-learning) para facilitar el acceso a todo el personal. La evaluación consistirá en un cuestionario final de 10 preguntas, requiriendo una nota mínima de 70/100 para la obtención del certificado, el cual será indispensable para la gestión de credenciales de TI.

Módulo 2: Identificación de vulnerabilidades y ciberseguridad operativa

- Justificación empírica: A pesar de que los colaboradores perciben el riesgo, el nivel de "Capacidad para identificar vulnerabilidades" (D5: media = 3,33) es solo moderado. Este módulo busca elevar esa capacidad de reactiva a proactiva.
- Objetivo y duración: Al finalizar este módulo de 6 horas, el personal con acceso a datos sensibles será capaz de aplicar técnicas de supervisión humana

(*human-in-the-loop*), identificar sesgos y "alucinaciones" en los resultados algorítmicos, y aplicar el protocolo de reporte de incidentes.

- Contenidos: El programa se enfoca en: (a) vectores de ataque por IA generativa (phishing, inyección de código); (b) ejercicios prácticos de clasificación de información; y (c) la ejecución paso a paso del Formulario de Incidente de Seguridad (FIS-001).
- Metodología y evaluación: Se realizarán talleres prácticos con simulaciones de casos reales. La evaluación se basará en la resolución de dilemas éticos y de seguridad, aprobando por competencia demostrada.

Módulo 3: Gobernanza de IA para líderes y tomadores de decisiones

- Justificación empírica: La ausencia total de *expertise* avanzado (0% en D3) evidencia que ni siquiera los líderes poseen el conocimiento necesario para gobernar la IA. Este módulo está diseñado para ellos.
- Objetivo y duración: Al finalizar este seminario ejecutivo de 3 horas, los gerentes, jefes de área y responsables de TI comprenderán los marcos de referencia internacionales (ISO/IEC 42001, NIST AI RMF) y el "deber de prudencia tecnológica" que les compete como líderes.
- Contenidos: Incluye: (a) análisis de la norma ISO/IEC 42001:2023; (b) el ciclo de gestión de riesgos del NIST (Mapear, Medir, Gestionar, Gobernar); y (c) el diseño y auditoría de políticas internas.
- Metodología y evaluación: Se impartirá como un seminario ejecutivo. La evaluación consistirá en la entrega de un plan de acción para implementar el marco de gobernanza en sus respectivas áreas.

Plan de implementación

Para garantizar que el Marco de Gobernanza de Inteligencia Artificial (MGAI-LF v1.0) se integre de manera exitosa en la cultura y operaciones de La Fabril S.A., se ha diseñado un plan de implementación estructurado en tres fases progresivas. Este despliegue abarca un horizonte temporal de doce meses y requiere la colaboración conjunta entre la Alta Gerencia, el Departamento de Tecnologías de la Información (TI) y la Dirección de Talento Humano. A continuación, en la Tabla 19, se detalla el cronograma de ejecución estratégico.

Tabla 19

Fases de implementación del Marco de Gobernanza de IA en La Fabril S.A.

Fase y plazo	Actividades clave	Responsables principales	KPI's de seguimiento
Fase 1: Preparación y Aprobación (0–3 meses)	• Constitución del Comité de Gobernanza de IA.• Aprobación y difusión de la Política de Uso Aceptable.• Clasificación inicial de información crítica. • Ejecución del Módulo 1 de capacitación.	TI, RRHH y Gerencia General	• % de colaboradores capacitados en M1 ≥ 90%.• Política publicada en intranet.
Fase 2: Ejecución y Despliegue (3–6 meses)	• Implementación del sistema de clasificación de datos.• Ejecución del Módulo 2 para personal con acceso a datos sensibles.• Auditoría inicial de herramientas de IA en uso (*Shadow AI*).	Comité de Gobernanza y TI	• % de personal M2 certificado ≥ 80%.• Inventario de herramientas completado.
Fase 3: Auditoría y Mejora Continua (6–12 meses)	• Ejecución del Módulo 3 para líderes.• Primera auditoría de cumplimiento del marco.• Actualización de políticas y reporte anual al directorio.	Comité de Gobernanza y Dirección	• Reporte de auditoría emitido.• % de no conformidades resueltas ≥ 85%.

Nota. La ejecución de este plan requerirá la asignación de un presupuesto operativo por parte de la Alta Gerencia para la adquisición de plataformas de E-learning y licencias de software.

Conformación del comité de gobernanza de IA

El éxito de este marco depende de la creación de un órgano ejecutivo responsable de su supervisión. El Comité de Gobernanza de IA debe estar integrado por: el Director de TI (quien lo presidirá), el Jefe de Recursos Humanos, el Responsable de Seguridad de la Información y un representante de la Gerencia General. Sus funciones principales serán: (a) aprobar o denegar el uso de nuevas herramientas de IA, (b) revisar los incidentes de seguridad reportados (FIS-001), (c) actualizar las políticas anualmente, y (d) emitir el reporte de gobernanza para el directorio de la compañía.

Impacto esperado y viabilidad

La ejecución del Marco de Gobernanza (MGAI-LF v1.0) proyecta una disminución drástica de los riesgos asociados al uso empírico y no regulado de la Inteligencia Artificial dentro de La Fabril S.A., estructurando sus beneficios en tres horizontes temporales. A corto plazo, la impartición del primer módulo de capacitación buscará elevar el nivel de claridad ética del personal (D1), proyectando un incremento desde la media actual de 2,64 hacia un estándar de seguridad operativo superior a los 3,50 puntos; este avance podrá ser verificado al replicar el cuestionario de esta investigación tras un semestre de ejecución. A mediano plazo, el objetivo central es neutralizar el principal factor de riesgo humano al reducir el índice de colaboradores sin instrucción técnica (actualmente en un 21,98%) a una cifra inferior al 5% de la plantilla. Finalmente, a largo plazo, el asentamiento operativo del Comité de Gobernanza de IA permitirá que la compañía se consolide como un referente de madurez digital y ética corporativa dentro de la industria manufacturera ecuatoriana.

Desde la perspectiva de la viabilidad, esta propuesta se destaca por tres factores estratégicos que garantizan su factibilidad inmediata. Primero, a nivel tecnológico y financiero, La Fabril S.A. ya cuenta con acceso operativo a herramientas como Gemini

Workspace, lo cual elimina la necesidad de realizar inversiones económicas adicionales en infraestructura base. Segundo, a nivel cultural, existe un respaldo casi total por parte de la fuerza laboral (98,28%) hacia la formalización de normativas (D10: media = 4,64), asegurando una adopción orgánica y libre de la habitual resistencia al cambio. Tercero, en el ámbito político e institucional, el diseño del marco se articula directamente con las exigencias de la Estrategia Nacional de Inteligencia Artificial del país (MINTEL, 2026), convirtiendo a la empresa en un caso pionero de cumplimiento normativo voluntario que puede servir de modelo para todo el sector privado.

Anexo C

Correo de autorización para el proyecto de titulación

Bryan Velez

De: Kevin Zambrano
Enviado el: lunes, 27 de julio de 2026 19:44
Para: Bryan Velez
CC: Bayron Ormaza
Asunto: RE: Solicitud de Aprobación Propuesta Metodológica

Hola Bryan

De lo revisado sobre el material para la realización de la encuesta veo que cumple lo que indicas, por lo que puedes proceder.

Cualquier apoyo nos comentas.

Saludos

De: Bryan Velez <bvelez@lafabril.com.ec>
Enviado: lunes, 27 de julio de 2026 11:03
Para: Kevin Zambrano <kzambrano@lafabril.com.ec>; Bayron Ormaza <bormaza@lafabril.com.ec>
Asunto: Solicitud de Aprobación Propuesta Metodológica

Estimados,

Byron / Kevin buen día,

Por medio de la presente, solicito de su aprobación para dar continuidad a mi proyecto de titulación, el cual tiene como modalidad un caso de estudio y emplea un cuestionario anónimo aplicado a una muestra aleatoria de colaboradores, con el objetivo de conocer la percepción sobre el uso de la inteligencia artificial en la transformación digital.

La información es utilizada exclusivamente con fines académicos, garantizando la confidencialidad de los participantes y sin divulgar información sensible o confidencial de la empresa.

Quedo atento a su gentil respuesta.

1

Este mensaje contiene información PRIVILEGIADA y CONFIDENCIAL. Está destinado exclusivamente al uso de la persona o personas a quienes aparece dirigido. Si este mensaje no está dirigido a usted o le ha llegado por error, sírvase tomar nota de que cualquier revisión, difusión o duplicación de esta comunicación queda estrictamente PROHIBIDA. Si usted no es la persona a quien el presente mensaje va dirigido, por favor contacte a LA FABRIL S.A., respondiendo este mensaje y destruya todas las copias del mismo. Muchas gracias. This message contains PRIVILEGED and CONFIDENTIAL information. It is intended only for the use of the person(s) to which it has been addressed. If you are not the intended recipient or have received it by mistake, please be advised that any review, dissemination, distribution or duplication of this communication is strictly PROHIBITED. If you are not the intended recipient, please contact LA FABRIL by reply email and destroy all copies of the original message. Thank you.