



Universidad
Europea

Integración de la Inteligencia Artificial en los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST)

Trabajo Fin de Máster (TFM)

Master universitario en sistemas integrados de gestión

Cristian Alejandro Espinoza Sanhueza

Universidad Europea (UE)
Fecha: 17 de mayo de 2026

Resumen (Español)

Este Trabajo Fin de Máster analiza la integración de la inteligencia artificial (IA) en los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST), abordando tanto su potencial preventivo como los riesgos técnicos, organizacionales, éticos y psicosociales asociados a su uso en entornos laborales. El estudio se fundamenta en la normativa internacional ISO 45001 como eje del sistema de gestión, complementada con marcos específicos de gobernanza y gestión de riesgos de la IA, tales como el NIST Artificial Intelligence Risk Management Framework, la norma ISO/IEC 23894 y la ISO/IEC 42001.

La metodología adoptada es de enfoque cualitativo-aplicado e incluye una revisión de literatura especializada, un análisis normativo comparado y el diseño de una propuesta operativa para la integración responsable de la IA en el SG-SST. Los resultados evidencian que la IA puede fortalecer la identificación y control de riesgos, facilitar la transición desde enfoques reactivos hacia estrategias preventivas y potenciar el aprendizaje organizacional, siempre que se integre de manera sistemática y gobernada, y no como una solución tecnológica aislada.

Como principal aporte, el trabajo propone un modelo de integración en ocho etapas alineado con el ciclo PHVA, acompañado de una matriz de riesgos y controles, indicadores clave de desempeño y un modelo de madurez organizacional. Esta propuesta se aplica a un caso práctico del sector de obras menores de construcción en Chile, considerando la normativa legal vigente y la participación de los trabajadores. Se concluye que la integración efectiva de la IA en los SG-SST es viable y auditable bajo estándares internacionales, siempre que se priorice la centralidad de las personas, la transparencia, la privacidad y el rol estratégico del profesional de EHS en la transformación digital.

Abstract (English)

This Master's Thesis analyzes the integration of artificial intelligence (AI) into Occupational Safety and Health Management Systems (OSH-MS), addressing both its preventive potential and the technical, organizational, ethical, and psychosocial risks associated with its use in workplace settings. The study is grounded in ISO 45001 as the backbone of the management system, complemented by international AI governance and risk management frameworks, including the NIST Artificial Intelligence Risk Management Framework, ISO/IEC 23894, and ISO/IEC 42001.

A qualitative and applied methodological approach was adopted, combining a literature review, a comparative normative analysis, and the design of an operational proposal for the responsible integration of AI into OSH-MS. The findings indicate that AI can enhance hazard identification and risk control, support the transition from reactive to preventive management approaches, and strengthen organizational learning, provided that it is integrated in a structured and governed manner rather than implemented as isolated technological solutions.

The main contribution of this thesis is an eight-stage integration model aligned with the PDCA cycle, supported by a risk and control matrix, key performance indicators, and an organizational maturity model. The proposal is applied to a practical case study in the small-scale construction sector in Chile, considering local legal requirements and worker participation. The study concludes that the effective integration of AI into OSH-MS is feasible and auditable under international standards, as long as it prioritizes a human-centered approach, transparency, data protection, and the strategic role of the EHS professional in driving digital transformation.

Contenido

Capítulo 1. Introducción.....	1
1.1 Contexto y oportunidad	2
1.2 Planteamiento del problema.....	3
1.3 Justificación	3
1.5 Alcance	4
Capítulo 2. Objetivos.....	4
2.1 Objetivo general y objetivos específicos.....	4
2.2 Objetivos específicos.....	4
Capítulo 3. Marco teórico	4
3.1 Seguridad y Salud en el Trabajo y los Sistemas de Gestión.....	4
3.2 ISO 45001 y el ciclo PHVA (PDCA).....	5
3.3 Inteligencia Artificial: conceptos fundamentales.....	5
3.4 Aplicaciones de la IA en Seguridad y Salud en el Trabajo.....	6
3.5 Riesgos y limitaciones de la IA en entornos laborales.....	7
3.6 Factores humanos, ergonomía cognitiva y aceptación.....	7
3.7 Síntesis del marco teórico.....	8
Capítulo 4. Marco normativo y técnico para la integración de la IA en el SG-SST	8
4.1 Importancia del marco normativo en la integración de la IA.....	8
4.2 ISO 45001 como eje del Sistema de Gestión de SST	9
4.3 Gestión de riesgos de IA: NIST AI Risk Management Framework 1.0	9
4.4 ISO/IEC 23894: gestión de riesgos de IA a lo largo del ciclo de vida	10
4.5 ISO/IEC 42001: sistema de gestión de la inteligencia artificial	10
4.6 Principios internacionales de IA responsable: OCDE y OIT	11
4.7 Marco legal chileno aplicable a la SST y la IA.....	11
4.8 Síntesis del marco normativo y técnico	12
Capítulo 5. Metodología	12
5.1 Enfoque metodológico.....	12
5.2 Diseño de la revisión de literatura	13
5.3 Estrategia de búsqueda y fuentes de información	13
5.4 Criterios de inclusión y exclusión	14
5.5 Proceso de selección y síntesis de la información	14
5.6 Análisis normativo comparado	15



5.7 Consideraciones éticas y psicosociales	15
5.8 Diseño del caso práctico	16
5.9 Síntesis metodológica	17
Capítulo 6. Resultados y análisis	17
6.1 Introducción al análisis de resultados.....	17
6.2 Beneficios del uso de la IA en la gestión de la SST.....	17
6.3 Riesgos y limitaciones de la IA aplicada a la SST	18
6.4 Análisis comparado por tecnología de IA	19
6.5 Trazabilidad entre ISO 45001 y los marcos de gobernanza de IA.....	20
6.6 Implicancias para el rol del profesional EHS	21
6.7 Síntesis de resultados	22
Capítulo 7. Propuesta de integración de la inteligencia artificial en el SG-SST	22
7.1 Introducción a la propuesta de integración	22
7.2 Principios rectores de la integración de IA en SST	22
7.3 Proceso de integración de la IA en el SG-SST	23
7.4 Roles y responsabilidades	26
7.5 Matriz de riesgos, controles y métricas.....	26
7.6 Indicadores clave de desempeño (KPI)	27
7.7 Modelo de madurez para la integración de IA en SST	29
7.8 Síntesis de la propuesta	30
Capítulo 8. Caso práctico: integración de IA en obras menores de construcción (Chile)	30
8.1 Contexto y alcance del caso	30
8.2 Objetivos y metas del piloto.....	30
8.3 Diseño metodológico del caso (cuasi-experimental).....	31
8.4 Componentes tecnológicos y flujo de datos.....	32
8.5 Gestión de riesgos, privacidad y relaciones laborales.....	32
8.6 Plan de implementación (12 meses) y gestión del cambio	33
8.7 Indicadores y tablero (definiciones operacionales).....	34
8.8 Evaluación de impacto y análisis económico	36
8.9 Resultados esperados y criterios de cierre.....	36
8.10 Riesgos residuales y planes de contingencia.....	37
8.11 Síntesis del caso	37
Capítulo 9. Conclusiones y líneas futuras	37



9.1 Síntesis de hallazgos	37
9.2 Conclusiones principales	38
9.3 Recomendaciones prácticas para la implantación	39
9.4 Implicancias para el rol del profesional EHS	39
9.5 Limitaciones del estudio.....	39
9.6 Líneas futuras de trabajo.....	40
9.7 Cierre y aportes	40
9.7.1 Aportes del TFM.....	40
Capítulo 10. Anexos	41
Anexo A. Política de Inteligencia Artificial en Seguridad y Salud en el Trabajo	42
Anexo B. Procedimiento Operativo Estándar (SOP) – Integración de IA en el SG-SST	43
Anexo C. Plantilla de Evaluación de Impacto de IA (EIIA)	43
Anexo D. Matriz de riesgos de IA aplicada a SST (ISO/IEC 23894)	45
Anexo E. Indicadores clave de desempeño (KPIs) y tablero	45
Anexo F. Checklist de evaluación de proveedores de IA.....	46
Anexo G. Modelo de consentimiento informado para trabajadores.....	46
1. Integrar la IA como parte del sistema de gestión, no como solución aislada	47
2. Establecer una gobernanza clara de la IA aplicada a SST	48
3. Priorizar casos de uso con alto valor preventivo y bajo impacto negativo	48
4. Incorporar la Evaluación de Impacto de IA como práctica estándar	48
5. Asegurar la participación y comunicación con los trabajadores	48
6. Definir y monitorear indicadores técnicos y preventivos relevante	49
7. Fortalecer el rol del profesional EHS frente a la transformación digital.....	49
8. Promover la mejora continua y el aprendizaje organizacional	49
Capítulo 11. Referencias	49

Capítulo 1. Introducción

La transformación digital de las organizaciones ha impulsado la incorporación progresiva de tecnologías avanzadas en los procesos productivos y de gestión. Entre ellas, la inteligencia artificial (IA) se ha consolidado de a poco como una herramienta con alto potencial para el análisis de grandes volúmenes de datos, la identificación de patrones complejos y el apoyo a la toma de decisiones en contextos dinámicos. En el ámbito de la Seguridad y Salud en el Trabajo (SST), estas capacidades abren la posibilidad de fortalecer los enfoques preventivos tradicionales, evolucionando desde modelos predominantemente reactivos hacia estrategias predictivas y proactivas orientadas a la anticipación del riesgo y así tener un control e eliminación de riesgos críticos.

Sin embargo, la introducción de la IA en entornos laborales no está exenta de desafíos. Más allá de los aspectos tecnológicos, su aplicación puede generar riesgos técnicos, organizacionales, éticos y psicosociales, especialmente cuando implica el tratamiento de datos personales, el monitoreo de actividades laborales o la automatización parcial de decisiones con impacto en la seguridad y la salud de los trabajadores. En este contexto, uno de los principales problemas identificados en la práctica es que muchas iniciativas de IA se desarrollan como proyectos tecnológicos aislados, sin una integración sistemática en los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST), lo que limita su efectividad preventiva y dificulta su control, evaluación y auditoría.

La norma ISO 45001 establece un marco internacionalmente reconocido para la gestión de la SST, basado en el liderazgo, la participación de los trabajadores, el enfoque de procesos y la mejora continua. Su estructura permite integrar nuevas tecnologías siempre que se mantenga la coherencia con los principios preventivos y el cumplimiento de los requisitos legales aplicables. No obstante, ISO 45001 no aborda de forma específica los riesgos asociados a la inteligencia artificial, lo que hace necesario complementar el SG-SST con marcos técnicos y normativos orientados a la gestión y gobernanza de la IA, tales como el NIST Artificial Intelligence Risk Management Framework y las normas ISO/IEC 23894 e ISO/IEC 42001.

En este escenario, el presente Trabajo Fin de Máster tiene como propósito analizar y proponer una forma estructurada, responsable y auditable de integrar la inteligencia artificial dentro de los Sistemas de Gestión de Seguridad y Salud en el Trabajo. El trabajo adopta un enfoque aplicado, orientado a conectar la normativa de SST con los marcos internacionales de gestión de riesgos y gobernanza de la IA,

incorporando además factores humanos, consideraciones éticas y aspectos psicosociales como elementos centrales del proceso de integración.

La investigación se apoya en una revisión de literatura especializada, un análisis normativo comparado y el diseño de una propuesta operativa que se materializa en un modelo de integración, matrices de riesgos y controles, indicadores de desempeño y un caso práctico contextualizado al sector de obras menores de construcción en Chile. Este enfoque permite no solo abordar el potencial preventivo de la IA, sino también establecer límites claros para su uso, resguardar los derechos de los trabajadores y asegurar que las decisiones apoyadas por sistemas inteligentes mantengan siempre el criterio profesional y la responsabilidad organizacional.

De este modo, el TFM busca contribuir tanto al ámbito académico como a la práctica profesional en EHS, proporcionando una guía que facilite la adopción de la inteligencia artificial como una herramienta de apoyo a la gestión preventiva, integrada al SG-SST, alineada con estándares internacionales y orientada a la mejora continua del desempeño en seguridad y salud en el trabajo (SST)

1.1 Contexto y oportunidad

La acelerada digitalización de los procesos productivos ha habilitado el uso de sistemas de inteligencia artificial (IA) capaces de reconocer patrones, anticipar eventos y apoyar decisiones en tiempo real. En Seguridad y Salud en el Trabajo (SST), la IA abre la posibilidad de evolucionar desde un enfoque predominantemente reactivo —basado en la investigación posterior al incidente— hacia un paradigma preventivo y predictivo, sin perder los principios de liderazgo, participación de trabajadores y mejora continua que exige ISO 45001 (ISO, 2018). En sectores como las obras menores de construcción y del área industrial caracterizados por alta variabilidad de frentes de trabajo, subcontratación y coexistencia de múltiples actividades, la IA resulta especialmente prometedora para mejorar la identificación de peligros, el control operacional y la priorización dinámica de recursos de control.

En este contexto, tecnologías como visión por computador (para verificación de EPP, intrusiones en zonas de exclusión y posturas inseguras), analítica predictiva (para priorización de riesgos) y procesamiento de lenguaje natural (PLN) (para explotar reportes y hallazgos) han pasado de prototipos a implementaciones reales. El desafío, no obstante, consiste en integrarlas de forma responsable y auditable dentro del SG-SST, asegurando confiabilidad, explicabilidad, privacidad y equidad.

1.2 Planteamiento del problema

Pese a la proliferación de soluciones comerciales, las organizaciones reportan dudas sobre (a) confiabilidad y desempeño sostenido de los modelos; (b) explicabilidad para la toma de decisiones; (c) sesgos derivados de datos de entrenamiento; (d) privacidad y límites del monitoreo; y (e) aceptación por parte de supervisores y cuadrillas. En entornos de construcción e industriales—donde las condiciones cambian rápidamente— esto se acentúa por la rotación de personal, heterogeneidad de contratistas y variabilidad de iluminación/ángulos para visión por computador.

Problema de investigación: ¿Cómo integrar la IA en el SG-SST de manera responsable, medible y efectiva, garantizando trazabilidad con ISO 45001 y habilitando auditorías cruzadas con ISO/IEC 42001?

1.3 Justificación

La evidencia reciente sugiere que la IA puede reducir incidentes y mejorar el cumplimiento cuando se diseña, valida y gobierna con estándares robustos (EU-OSHA, 2022; NIOSH, 2024). Sin embargo, muchas iniciativas fracasan por tratar la IA como un **“proyecto tecnológico”** desacoplado de los procesos y roles del SG-SST. Este Trabajo Fin de Máster (TFM) aporta una guía práctica y auditable para integrar la IA dentro del sistema de gestión, conectando ISO 45001 con marcos de gestión de riesgos de IA (NIST AI RMF 1.0, ISO/IEC 23894) y con un sistema de gestión de IA (ISO/IEC 42001). El resultado es un enfoque sistémico que abarca personas, procesos y tecnología, y que puede demostrarse mediante evidencias, métricas y auditorías integradas.

Aplicar la propuesta a un caso práctico del sector de obras menores en Chile, considerando normativa local.

1.5 Alcance

Alcance. El TFM cubre el ciclo de vida de la IA (ideación - diseño - verificación/validación - despliegue controlado - operación y monitoreo - mejora) y su integración con procesos del SG-SST (identificación de peligros, planificación, operación, evaluación del desempeño y mejora). Se consideran lineamientos de privacidad, ética y el marco legal chileno (Ley 16.744; DS 594; Ley 19.628).

Capítulo 2. Objetivos

2.1 Objetivo general y objetivos específicos

Objetivo general. Proponer recomendaciones para una integración efectiva de la IA en los SG-SST, considerando buenas prácticas y estándares internacionales (ISO 45001; NIST AI RMF; ISO/IEC 23894; ISO/IEC 42001), y el rol del profesional EHS.

2.2 Objetivos específicos.

Definir un proceso de integración de IA en ocho etapas con entregables y criterios de aceptación.

Desarrollar una matriz de riesgos y controles para tecnologías de IA aplicadas a SST, incluyendo métricas de desempeño técnico y sociotécnico.

Diseñar un modelo de madurez (niveles 1–5) para evaluar el progreso organizacional.

Proponer indicadores clave (KPI) técnicos, organizacionales y sociotécnicos para evaluación continua y auditoría.

Capítulo 3. Marco teórico

3.1 Seguridad y Salud en el Trabajo y los Sistemas de Gestión

La Seguridad y Salud en el Trabajo (SST) constituye un campo multidisciplinario orientado a la prevención de lesiones, enfermedades profesionales y daños a la salud derivados del trabajo. Su evolución ha

transitado desde enfoques normativos y reactivos hacia modelos sistémicos, basados en la identificación de peligros, evaluación de riesgos y mejora continua. En este contexto, los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST) se consolidan como el marco organizacional que articula políticas, procesos, responsabilidades y recursos para controlar los riesgos laborales de manera estructurada y verificable.

La norma ISO 45001:2018 establece los requisitos para implementar un SG-SST eficaz, alineado con otros sistemas de gestión ISO y sustentado en el ciclo Planificar-Hacer-Verificar-Actuar (PHVA/PDCA). Este enfoque permite integrar nuevas tecnologías —incluida la inteligencia artificial— siempre que se mantenga el liderazgo de la alta dirección, la participación de los trabajadores y el cumplimiento de los requisitos legales aplicables (ISO, 2018).

3.2 ISO 45001 y el ciclo PHVA (PDCA)

ISO 45001 estructura el SG-SST en cuatro fases interrelacionadas:

Planificar (Plan): comprensión del contexto organizacional, liderazgo, consulta y participación de los trabajadores, identificación de peligros, evaluación de riesgos y determinación de controles.

Hacer (Do): provisión de recursos, competencia, concienciación, comunicación y control operacional.

Verificar (Check): seguimiento, medición del desempeño, auditorías internas e investigación de incidentes.

Actuar (Act): acciones correctivas y mejora continua del sistema.

La integración de tecnologías de IA debe alinearse con estas fases, de modo que los sistemas inteligentes no sustituyan el juicio profesional, sino que lo refuercen con información oportuna y trazable. ISO 45001 enfatiza además la necesidad de participación efectiva de los trabajadores, aspecto crítico para la aceptación de soluciones basadas en IA y para evitar impactos psicosociales negativos (ISO, 2018).

3.3 Inteligencia Artificial: conceptos fundamentales

La inteligencia artificial puede definirse como el conjunto de técnicas que permiten a los sistemas informáticos realizar tareas que normalmente requieren inteligencia humana, tales como reconocer

patrones, aprender de datos, razonar o tomar decisiones bajo incertidumbre. En el ámbito organizacional, la IA se implementa principalmente mediante las siguientes familias tecnológicas:

- a) Aprendizaje automático (Machine Learning, ML): algoritmos que aprenden patrones a partir de datos históricos para clasificar, predecir o priorizar eventos.
- b) Aprendizaje profundo (Deep Learning): subcampo del ML basado en redes neuronales profundas, ampliamente utilizado en visión por computador.
- c) Visión por computador: análisis automático de imágenes y video para detectar objetos, comportamientos o condiciones específicas.
- d) Procesamiento de Lenguaje Natural (PLN): técnicas para analizar texto libre, como reportes de incidentes, observaciones de seguridad o auditorías.

Estas tecnologías permiten procesar grandes volúmenes de información y detectar relaciones que serían difíciles de identificar mediante métodos tradicionales, lo que las hace particularmente atractivas para la gestión preventiva en SST (NIST, 2023).

3.4 Aplicaciones de la IA en Seguridad y Salud en el Trabajo

En el ámbito de la SST, las aplicaciones más relevantes de la IA incluyen:

- a) Identificación y control de riesgos: sistemas de visión por computador para verificar uso de equipos de protección personal (EPP), detectar intrusiones en zonas peligrosas o identificar posturas inseguras.
- b) Analítica predictiva de incidentes: modelos que priorizan riesgos o frentes de trabajo con mayor probabilidad de accidentes, apoyando la asignación de recursos preventivos.
- c) Gestión del conocimiento y aprendizaje organizacional: uso de PLN para analizar reportes de incidentes, near-miss y hallazgos de auditoría, reduciendo el subregistro y acelerando el aprendizaje.
- d) Robótica y automatización colaborativa: reducción de la exposición humana a tareas peligrosas, siempre que se implementen resguardos funcionales y evaluaciones de seguridad.

La evidencia internacional indica que estas aplicaciones pueden contribuir a reducciones significativas de incidentes cuando se implementan de forma focalizada y con participación de los trabajadores (EU-OSHA, 2022; NIOSH, 2024).

3.5 Riesgos y limitaciones de la IA en entornos laborales

Pese a su potencial, la IA introduce riesgos emergentes que deben ser gestionados explícitamente dentro del SG-SST:

- Sesgos algorítmicos: derivados de datos incompletos o no representativos, que pueden generar decisiones injustas o ineficaces.
- Opacidad o falta de explicabilidad: dificultad para comprender cómo un modelo llega a una recomendación, lo que afecta la confianza y la rendición de cuentas.
- Riesgos de privacidad y protección de datos: especialmente relevantes cuando se utilizan imágenes, videos o datos personales de trabajadores.
- Dependencia excesiva de la automatización: que puede conducir al sesgo de automatización, reduciendo la vigilancia humana crítica.

Estos riesgos justifican la necesidad de integrar la IA bajo marcos de gestión de riesgos específicos, como el NIST AI Risk Management Framework y la ISO/IEC 23894, en coherencia con el SG-SST (NIST, 2023; ISO/IEC, 2023a).

3.6 Factores humanos, ergonomía cognitiva y aceptación

La integración de IA en SST constituye un cambio sociotécnico, no solo tecnológico. La ergonomía cognitiva estudia cómo las personas interactúan con sistemas complejos y resulta clave para evitar:

- Fatiga de alertas, cuando los sistemas generan excesivas notificaciones.
- Sesgo de automatización, cuando los usuarios confían ciegamente en la recomendación del sistema.
- Rechazo organizacional, cuando la IA es percibida como una herramienta de vigilancia o control disciplinario. Por eso la importancia de la educación de la IA en los trabajadores.

La literatura destaca que la aceptación de sistemas de IA depende de la transparencia sobre su propósito, límites claros de uso, participación temprana de los trabajadores y retroalimentación útil para la toma de decisiones (EU-OSHA, 2022; OIT, 2024).

3.7 Síntesis del marco teórico

En síntesis, el marco teórico evidencia que la IA puede fortalecer la gestión preventiva en SST si y solo si se integra dentro de un SG-SST robusto, alineado con ISO 45001 y complementado por marcos de gestión de riesgos y gobernanza de IA. La combinación de tecnología, factores humanos y gobernanza constituye la base conceptual sobre la cual se desarrolla la propuesta de integración presentada en los capítulos siguientes.

Capítulo 4. Marco normativo y técnico para la integración de la IA en el SG-SST

4.1 Importancia del marco normativo en la integración de la IA

La integración de la inteligencia artificial en la gestión de la seguridad y salud en el trabajo no puede abordarse únicamente desde una perspectiva tecnológica. Dado que las decisiones apoyadas por IA pueden influir directamente en la seguridad física, la salud y los derechos fundamentales de los trabajadores, resulta indispensable contar con un marco normativo y técnico sólido que oriente su diseño, implementación y operación.

En este sentido, los estándares internacionales cumplen una doble función: por una parte, reducen la incertidumbre asociada a tecnologías emergentes y, por otra, permiten demostrar cumplimiento y diligencia ante organismos fiscalizadores, auditorías internas y partes interesadas. La adopción de la IA en SST debe, por tanto, integrarse de manera coherente con los sistemas de gestión existentes, especialmente con ISO 45001, y complementarse con marcos específicos de gestión de riesgos de IA y gobernanza tecnológica.

4.2 ISO 45001 como eje del Sistema de Gestión de SST

La norma ISO 45001:2018 constituye el principal referente internacional para la implementación de sistemas de gestión de seguridad y salud en el trabajo. Su enfoque basado en procesos y en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) permite integrar nuevas tecnologías sin desvirtuar los principios fundamentales de la gestión preventiva.

Desde la perspectiva de la IA, ISO 45001: 2018 aporta elementos clave:

- Liderazgo y compromiso de la alta dirección en la adopción responsable de tecnologías.
- Participación y consulta de los trabajadores, requisito crítico cuando se introducen sistemas de monitoreo o análisis automatizado.
- Identificación de peligros y evaluación de riesgos, procesos donde la IA puede actuar como herramienta de apoyo, pero no como sustituto del juicio profesional.
- Evaluación del desempeño y mejora continua, que facilitan la medición del impacto real de las soluciones basadas en IA.

La norma no prescribe tecnologías específicas, lo que permite que la IA sea incorporada de forma flexible, siempre que se mantenga la coherencia con los objetivos del SG-SST y el cumplimiento legal aplicable.

4.3 Gestión de riesgos de IA: NIST AI Risk Management Framework 1.0

El NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) proporciona un enfoque estructurado para identificar, evaluar y gestionar los riesgos asociados a sistemas de IA a lo largo de su ciclo de vida. Este marco resulta especialmente relevante para el ámbito laboral, donde los riesgos de la IA pueden tener consecuencias directas sobre las personas trabajadoras.

El NIST AI RMF se organiza en cuatro funciones interrelacionadas:

- GOVERN (Gobernar): establecimiento de políticas, roles y responsabilidades para la IA.
- MAP (Mapear): comprensión del contexto, los casos de uso y las partes interesadas.
- MEASURE (Medir): evaluación de riesgos, desempeño y efectos adversos.
- MANAGE (Gestionar): tratamiento de riesgos, monitoreo y mejora continua.

Estas funciones son altamente compatibles con el enfoque PHVA de ISO 45001, lo que facilita su integración dentro del SG-SST. Por ejemplo, GOVERN se alinea con liderazgo y política; MAP con planificación y evaluación de riesgos; MEASURE con seguimiento del desempeño; y MANAGE con acciones correctivas y mejora (NIST, 2023).

4.4 ISO/IEC 23894: gestión de riesgos de IA a lo largo del ciclo de vida

La norma ISO/IEC 23894:2023 complementa el NIST AI RMF al proporcionar directrices específicas para la gestión de riesgos de la IA durante todo su ciclo de vida, desde la concepción del sistema hasta su retiro.

Este estándar enfatiza:

- La identificación de riesgos técnicos (sesgos, errores de clasificación, fallos de desempeño).
- La consideración de riesgos organizacionales y humanos, incluidos impactos psicosociales.
- La necesidad de controles proporcionales al nivel de riesgo y criticidad del caso de uso.
- La documentación y trazabilidad de las decisiones relacionadas con la IA.

En el contexto de la SST, ISO/IEC 23894 permite estructurar evaluaciones como la Evaluación de Impacto de IA (EIIA), que integra aspectos técnicos, éticos y laborales, reforzando el principio de prevención (ISO/IEC, 2023a).

4.5 ISO/IEC 42001: sistema de gestión de la inteligencia artificial

La norma ISO/IEC 42001:2023 introduce un sistema de gestión específico para IA, similar en estructura a otros estándares ISO de sistemas de gestión. Su principal aporte es proporcionar un marco certificable para la gobernanza de la IA dentro de las organizaciones.

ISO/IEC 42001 establece requisitos para:

- Política y objetivos de IA.
- Gestión de riesgos y oportunidades asociados a sistemas de IA.
- Control del ciclo de vida de los sistemas.

- Competencia, concienciación y comunicación.
- Evaluación del desempeño y mejora del sistema de gestión de IA.

La compatibilidad estructural entre ISO 45001 e ISO/IEC 42001 permite implementar un enfoque integrado, donde la IA se gestiona como una capacidad organizacional y no como un conjunto de soluciones aisladas (ISO/IEC, 2023b).

4.6 Principios internacionales de IA responsable: OCDE y OIT

A nivel internacional, los Principios de IA de la OCDE y las directrices de la Organización Internacional del Trabajo (OIT) aportan un marco ético y social indispensable para el uso de IA en entornos laborales.

Los principios de la OCDE destacan que la IA debe ser:

- Centrada en las personas y el bienestar humano.
- Robusta, segura y confiable.
- Transparente y explicable.
- Responsable y sujeta a rendición de cuentas.

Por su parte, la OIT subraya que la digitalización y la IA deben contribuir al trabajo decente, evitando prácticas de vigilancia excesiva, discriminación o deterioro de la salud mental de los trabajadores (OCDE, 2019; OIT, 2024).

4.7 Marco legal chileno aplicable a la SST y la IA

En Chile, la integración de IA en SST debe considerar el siguiente marco normativo:

- Ley 16.744, que regula el seguro social contra accidentes del trabajo y enfermedades profesionales.
- Decreto Supremo N° 594, que establece las condiciones sanitarias y ambientales básicas en los lugares de trabajo.
- Ley 19.628, sobre protección de la vida privada y datos personales.
- Lineamientos y estadísticas de la Superintendencia de Seguridad Social (SUSESO) y protocolos del Instituto de Salud Pública (ISP).

La aplicación de IA no exime a la empresa de sus responsabilidades legales; por el contrario, exige mayor diligencia en materia de privacidad, proporcionalidad y participación de los trabajadores. Viene a complementar de manera estricta el control de accidentes en base a una estandarización ISO 45001 y normas locales de seguridad y salud en el trabajo.

4.8 Síntesis del marco normativo y técnico

El análisis normativo evidencia que la integración de la IA en el SG-SST es viable y consistente cuando se articula:

- ISO 45001 como eje del sistema de gestión de SST.
- NIST AI RMF e ISO/IEC 23894 para la gestión de riesgos de IA.
- ISO/IEC 42001 para la gobernanza y mejora del sistema de IA.
- Principios OCDE y OIT, junto con el marco legal chileno, como base ética y jurídica.

Esta convergencia normativa constituye el fundamento técnico sobre el cual se desarrolla la metodología y la propuesta de integración presentadas en los capítulos siguientes.

Capítulo 5. Metodología

5.1 Enfoque metodológico

El presente Trabajo Fin de Máster adopta un enfoque cualitativo-aplicado, con orientación descriptiva y propositiva, cuyo propósito es desarrollar una guía práctica y auditable para la integración de la inteligencia artificial en los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST).

La metodología combina tres componentes principales:

- Revisión de literatura con elementos sistemáticos, orientada a identificar beneficios, riesgos, controles y métricas asociadas al uso de IA en SST.
- Análisis normativo y técnico, centrado en estándares internacionales y marcos de gobernanza de IA.

- Diseño de una propuesta aplicada, materializada en un modelo de integración, matrices operativas y un caso práctico contextualizado al sector de obras menores de construcción en Chile.

Este enfoque metodológico permite vincular el marco teórico y normativo con una propuesta operativa, alineada con las exigencias académicas del TFM y con la práctica profesional en EHS.

5.2 Diseño de la revisión de literatura

Se desarrolló una revisión narrativa con elementos sistemáticos, adecuada para abordar un campo emergente como la aplicación de IA en SST (Seguridad y salud en el trabajo), donde coexisten investigaciones académicas, estándares técnicos y documentos institucionales.

La revisión se orientó a responder las siguientes preguntas guía:

¿Cuáles son las principales aplicaciones de la IA en SST reportadas en la literatura reciente?

¿Qué beneficios y limitaciones se han identificado en su implementación?

¿Qué riesgos técnicos, organizacionales y psicosociales se asocian al uso de IA en entornos laborales?

¿Qué controles y métricas se recomiendan para una integración responsable y efectiva?

5.3 Estrategia de búsqueda y fuentes de información

La búsqueda se realizó entre los años 2018 y 2026, considerando publicaciones en español e inglés, con el objetivo de capturar la evolución reciente del tema. Se priorizaron las siguientes fuentes:

- Estándares y normas internacionales: ISO 45001, ISO/IEC 23894, ISO/IEC 42001.
- Marcos y guías institucionales: NIST AI RMF 1.0, OCDE, OIT, EU-OSHA, NIOSH/CDC.
- Literatura académica revisada por pares, relacionada con IA, SST, factores humanos y ergonomía cognitiva.
- Documentos regulatorios y técnicos nacionales, relevantes para el contexto chileno (SUSESO, ISP, normativa sanitaria).

5.4 Criterios de inclusión y exclusión

Para asegurar la calidad y pertinencia de la información analizada, se definieron los siguientes criterios:

Criterios de inclusión.

- Publicaciones que aborden aplicaciones reales o potenciales de IA en SST.
- Documentos que analicen riesgos, impactos éticos o factores humanos asociados a la IA.
- Estándares, marcos técnicos y guías institucionales vigentes o recientemente actualizados.
- Estudios con claridad metodológica y aplicabilidad al contexto organizacional.

Criterios de exclusión.

- Opiniones o artículos sin respaldo metodológico o técnico.
- Publicaciones duplicadas o desactualizadas sin relevancia actual.
- Estudios enfocados exclusivamente en IA sin relación con entornos laborales o SST.

Criterios de inclusión y exclusión.

Criterios de inclusión	Criterios de exclusión
Aplicaciones de IA en SST con evidencia o potencial real	Opiniones sin respaldo técnico o metodológico
Análisis de riesgos técnicos, organizacionales y psicosociales	Duplicados o publicaciones obsoletas
Estándares y marcos (ISO, NIST, OCDE, OIT)	IA sin conexión con entornos laborales o SST
Estudios con claridad metodológica y aplicabilidad	

5.5 Proceso de selección y síntesis de la información

El proceso de selección se desarrolló en tres etapas:

1. Identificación inicial de documentos mediante búsquedas estructuradas en las fuentes definidas.
2. Cribado de títulos y resúmenes para evaluar pertinencia temática.
3. Revisión de texto completo de los documentos seleccionados, evaluando su contribución al objetivo del TFM.

Los resultados fueron sintetizados mediante tablas comparativas y matrices conceptuales, que permitieron identificar patrones comunes en beneficios, riesgos, controles y métricas. Este proceso sirvió de base para el desarrollo del Capítulo 5 (Resultados y análisis) y del Capítulo 6 (Propuesta de integración).

5.6 Análisis normativo comparado

De forma complementaria a la revisión de literatura, se realizó un análisis normativo comparado, con el objetivo de evaluar la compatibilidad y complementariedad entre:

- ISO 45001 (SG-SST)
- NIST AI RMF 1.0 (gestión de riesgos de IA)
- ISO/IEC 23894 (riesgos de IA a lo largo del ciclo de vida)
- ISO/IEC 42001 (sistema de gestión de IA)

Este análisis permitió construir una trazabilidad estructural entre los requisitos de gestión de SST y los marcos de gobernanza de IA, elemento central de la propuesta metodológica del TFM.

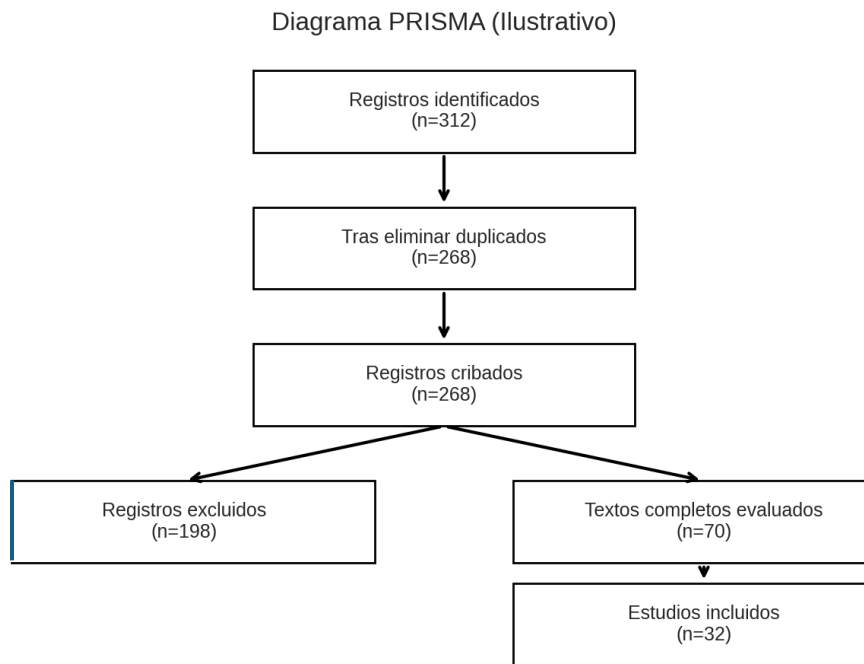
5.7 Consideraciones éticas y psicosociales

Dado que la IA aplicada a SST puede implicar el tratamiento de datos personales y el monitoreo de actividades laborales, se incorporaron consideraciones éticas desde la fase metodológica. En particular, se consideraron:

- Principios de IA centrada en las personas (OCDE).
- Enfoque de trabajo decente y prevención de riesgos psicosociales (OIT).
- Protección de datos personales y privacidad en el contexto chileno.

Como resultado, se incorporó el concepto de Evaluación de Impacto de IA (EIIA), entendida como una herramienta metodológica que integra aspectos técnicos, éticos y psicosociales, y que se desarrolla en detalle en la propuesta del Capítulo 6.

Diagrama PRISMA del proceso de selección (datos ilustrativos; reemplazar con recuentos reales).



5.8 Diseño del caso práctico

El caso práctico se diseñó con un enfoque aplicado y contextualizado, orientado al sector de obras menores de construcción en Chile. El diseño metodológico del caso considera:

- Identificación de riesgos críticos (caídas de altura, golpes, riesgos eléctricos).
- Selección de tecnologías de IA con evidencia de aplicabilidad (visión por computador y PLN).
- Definición de una línea base de indicadores de SST.
- Establecimiento de metas prudentes y medibles, basadas en la literatura.
- Consideración explícita de privacidad, participación de trabajadores y gestión del cambio.

Este diseño permite evaluar la viabilidad operativa de la propuesta y su alineación con el SG-SST.

5.9 Síntesis metodológica

La metodología empleada proporciona un marco coherente, replicable y alineado con estándares internacionales, que permite:

- Fundamentar teóricamente la integración de IA en SST.
- Analizar críticamente beneficios y riesgos.
- Diseñar una propuesta de integración auditable y aplicable.
- Contextualizar la propuesta en un escenario real del ámbito de la construcción.

Sobre esta base metodológica se presentan, en los capítulos siguientes, los resultados del análisis, la propuesta de integración y el caso práctico.

Capítulo 6. Resultados y análisis

6.1 Introducción al análisis de resultados

Este capítulo presenta los resultados derivados de la revisión de literatura, el análisis normativo y la síntesis metodológica desarrollados en los capítulos previos. El objetivo no es únicamente enumerar aplicaciones de la inteligencia artificial en la seguridad y salud en el trabajo (SST), sino analizar críticamente sus beneficios, riesgos, condiciones de éxito y limitaciones, así como su compatibilidad con los Sistemas de Gestión de SST (SG-SST) basados en ISO 45001.

El análisis se estructura en torno a tres ejes principales:

- Beneficios observados del uso de IA en SST.
- Riesgos y desafíos asociados a su implementación.
- Trazabilidad entre los marcos de gestión de SST y los marcos de gobernanza de IA.

6.2 Beneficios del uso de la IA en la gestión de la SST

La literatura revisada coincide en que la IA puede aportar valor significativo a la gestión preventiva cuando se utiliza como herramienta de apoyo a la toma de decisiones y no como sustituto del juicio humano. Los beneficios más relevantes se agrupan en las siguientes categorías:

6.2.1 Mejora en la identificación y control de riesgos

Las tecnologías de visión por computador permiten detectar de forma continua comportamientos inseguros, uso incorrecto o ausencia de equipos de protección personal (EPP), e intrusiones en zonas de riesgo. A diferencia de las inspecciones tradicionales, estas herramientas ofrecen monitoreo sistemático, reduciendo la dependencia exclusiva de observaciones puntuales.

Asimismo, la analítica predictiva basada en aprendizaje automático facilita la priorización de riesgos y frentes de trabajo con mayor probabilidad de incidentes, contribuyendo a una asignación más eficiente de recursos preventivos.

6.2.2 Transición desde enfoques reactivos a preventivos

Uno de los aportes más destacados de la IA es su capacidad para anticipar eventos antes de que se materialicen en accidentes. El análisis de patrones históricos de incidentes, near-miss y condiciones subestándar permite generar alertas tempranas y apoyar decisiones preventivas, alineándose con el enfoque proactivo promovido por ISO 45001.

6.2.3 Fortalecimiento del aprendizaje organizacional

El uso de procesamiento de lenguaje natural (PLN) para analizar reportes de incidentes, observaciones de seguridad y hallazgos de auditoría contribuye a reducir el subregistro y a identificar tendencias que podrían pasar desapercibidas en análisis manuales. Esto favorece la gestión del conocimiento y el aprendizaje organizacional continuo.

6.3 Riesgos y limitaciones de la IA aplicada a la SST

Pese a los beneficios identificados, los resultados del análisis evidencian que la implementación de IA en SST conlleva riesgos relevantes que deben ser gestionados explícitamente dentro del SG-SST.

6.3.1 Sesgos algorítmicos y calidad de los datos

Los modelos de IA dependen directamente de la calidad y representatividad de los datos utilizados para su entrenamiento. En entornos laborales dinámicos, como la construcción, los datos pueden estar incompletos o sesgados, generando falsos positivos o negativos que afectan la confiabilidad del sistema y la toma de decisiones.

6.3.2 Falta de explicabilidad y confianza

La opacidad de algunos modelos, especialmente los basados en aprendizaje profundo, dificulta comprender cómo se generan determinadas alertas o recomendaciones. Esta falta de explicabilidad puede erosionar la confianza de supervisores y trabajadores, y limita la rendición de cuentas en caso de incidentes.

6.3.3 Riesgos psicosociales y percepción de vigilancia

La percepción de monitoreo constante puede generar estrés, rechazo o resistencia por parte de los trabajadores si no se establecen límites claros de uso, objetivos preventivos explícitos y mecanismos de participación. Este aspecto resulta crítico desde la perspectiva de la SST y del trabajo decente promovido por la OIT.

6.3.4 Dependencia excesiva de la automatización

La literatura advierte sobre el sesgo de automatización, fenómeno en el cual los usuarios confían excesivamente en las recomendaciones del sistema, disminuyendo la vigilancia humana crítica. En SST, esta situación puede resultar particularmente peligrosa si se asume que la ausencia de alertas equivale a ausencia de riesgos.

6.4 Análisis comparado por tecnología de IA

Del análisis se desprende que no todas las tecnologías de IA presentan el mismo perfil de beneficios y riesgos:

- Visión por computador: alto potencial preventivo, pero elevada sensibilidad a condiciones ambientales y riesgos de privacidad.
- Analítica predictiva: útil para priorización estratégica, aunque dependiente de datos históricos de calidad.
- PLN: bajo nivel de intrusión y alto valor para aprendizaje organizacional, con riesgos relativamente menores.

Este hallazgo refuerza la necesidad de una selección cuidadosa de casos de uso, priorizando aquellos con mayor valor preventivo y menor impacto negativo.

Comparativo de tecnologías de IA en SST.

Tecnología	Beneficios en SST	Riesgos principales	Controles propuestos	Métricas sugeridas
Visión por computador	Verifica EPP, intrusiones, posturas	Privacidad; sensibilidad a iluminación/ángulos; falsas alertas	Anonimización; calibración; revisión humana	Precisión; Sensibilidad; FPR/FNR
Analítica predictiva	Priorización de riesgos y frentes	Opacidad; datos desbalanceados	Validación; explicabilidad; auditoría de datos	AUC; Lift; precisión/recall
PLN	Reduce subregistro y acelera aprendizaje	Ambigüedad semántica; confidencialidad	Taxonomías; control de accesos	Exactitud de clasificación; cobertura

6.5 Trazabilidad entre ISO 45001 y los marcos de gobernanza de IA

Uno de los resultados clave del análisis es la alta compatibilidad estructural entre ISO 45001 y los marcos de gestión de IA analizados. En particular, se identifican las siguientes correspondencias:

- Liderazgo y participación (ISO 45001) ↔ GOVERN (NIST AI RMF)
- Identificación de peligros y planificación ↔ MAP (NIST) e ISO/IEC 23894
- Control operacional y soporte ↔ MANAGE (NIST) e ISO/IEC 42001
- Seguimiento y evaluación del desempeño ↔ MEASURE (NIST) y auditoría de sistemas de IA
- Mejora continua ↔ Ciclo PHVA aplicado a la IA

Trazabilidad ISO 45001 ↔ NIST AI RMF ↔ ISO/IEC 23894 ↔ ISO/IEC 42001. (Auditable)

ISO 45001	NIST AI RMF	ISO/IEC 23894	ISO/IEC 42001	Evidencias ejemplo
Liderazgo y participación	GOVERN	—	—	Política de IA; RACI; actas
Planificación (peligros/riesgos)	MAP	Gestión de riesgos de IA	—	EIIA; registro de riesgos
Operación/Soporte	MANAGE	—	Gestión del ciclo de vida	SOP; registros de despliegue
Evaluación del desempeño	MEASURE	—	Auditoría del sistema	KPIs; auditorías internas
Mejora	Ciclo PHVA transversal	—	Mejora del sistema de IA	Lecciones aprendidas; revisión dirección

Esta trazabilidad permite integrar la IA dentro del SG-SST, evitando enfoques paralelos o desconectados y facilitando auditorías internas y externas.

6.6 Implicancias para el rol del profesional EHS

El análisis evidencia que la integración de la IA transforma el rol del profesional de EHS, quien pasa de ser únicamente un gestor de cumplimiento a desempeñar funciones clave como:

- Interlocutor entre tecnología y prevención, validando que los sistemas de IA respondan a objetivos de SST.
- Gestor de riesgos de IA, en coordinación con áreas de TI y legal.
- Facilitador del cambio organizacional, promoviendo la participación y aceptación de los trabajadores.
- Analista crítico de datos y métricas, evitando interpretaciones automáticas sin contexto.
- Educador de la incorporación de nuevas tecnologías en la organización.

6.7 Síntesis de resultados

En síntesis, los resultados del análisis muestran que la IA puede potenciar significativamente la gestión de la SST, siempre que se integre bajo un enfoque sistémico, participativo y gobernado. Los beneficios preventivos solo se materializan cuando se gestionan de forma explícita los riesgos técnicos, humanos y organizacionales.

Estos hallazgos fundamentan la propuesta de integración que se desarrolla orientada a operacionalizar la IA dentro del SG-SST de manera responsable, medible y alineada con estándares internacionales.

Capítulo 7. Propuesta de integración de la inteligencia artificial en el SG-SST

7.1 Introducción a la propuesta de integración

A partir de los resultados y análisis presentados en el Capítulo 5, se evidencia que la integración de la inteligencia artificial (IA) en la seguridad y salud en el trabajo solo genera valor sostenible cuando se implementa de manera sistémica, gobernada y alineada con el Sistema de Gestión de SST (SG-SST). En este contexto, el presente capítulo propone un modelo de integración operativa, diseñado para ser auditable, medible y compatible con los requisitos de ISO 45001, complementado con marcos específicos de gestión y gobernanza de IA.

La propuesta se estructura en torno a un proceso de ocho etapas, acompañado de roles claros, matrices de riesgos y controles, indicadores clave de desempeño (KPI) y un modelo de madurez que permite evaluar el nivel de adopción organizacional.

7.2 Principios rectores de la integración de IA en SST

La propuesta se fundamenta en los siguientes principios:

- IA como apoyo a la prevención, no como sustituto del criterio profesional.
- Centralidad de las personas, priorizando seguridad, salud, privacidad y bienestar.
- Proporcionalidad, aplicando mayores controles a casos de uso con mayor criticidad.
- Transparencia y explicabilidad, especialmente en decisiones con impacto en la SST.
- Participación de los trabajadores, desde el diseño hasta la operación.
- Mejora continua, mediante métricas, auditorías y retroalimentación.

Estos principios aseguran coherencia con ISO 45001, los Principios de IA de la OCDE y el enfoque de trabajo decente promovido por la OIT.

7.3 Proceso de integración de la IA en el SG-SST

Se propone un proceso de ocho etapas, integrable al ciclo PHVA del SG-SST:

Etapla 1. Identificación y priorización de casos de uso

Consiste en identificar oportunidades donde la IA aporte valor preventivo tangible. Los casos de uso deben priorizarse considerando:

- Gravedad del riesgo a controlar.
- Frecuencia de exposición.
- Factibilidad técnica.
- Impacto potencial en trabajadores.

Entregable: Catálogo de casos de uso priorizados.

Etapla 2. Análisis de contexto y partes interesadas

Se analiza el entorno organizacional, procesos afectados, trabajadores involucrados y expectativas de las partes interesadas, alineando el caso de uso con los objetivos del SG-SST.

Entregable: Análisis de contexto y matriz de partes interesadas.

Etapla 3. Evaluación de riesgos de IA (EIIA)

Se desarrolla una Evaluación de Impacto de IA, considerando:

- Riesgos técnicos (sesgos, errores, fallos).
- Riesgos organizacionales.
- Riesgos psicosociales.
- Privacidad y protección de datos.

Entregable: Registro de riesgos de IA y plan de tratamiento.

Etapas 4. Diseño del sistema y requisitos

Se definen requisitos de:

- Datos (calidad, minimización, seguridad).
- Desempeño del modelo.
- Explicabilidad.
- Interacción humano-sistema.

Entregable: Especificación técnica y funcional del sistema de IA.

Etapas 5. Verificación y validación (V&V)

Se valida el desempeño del sistema antes de su uso operativo, considerando pruebas técnicas y pruebas con usuarios reales.

Entregable: Informe de verificación y validación.

Etapas 6. Despliegue controlado y gestión del cambio

El sistema se implementa de forma gradual, acompañado de:

- Capacitación.
- Comunicación transparente.
- Gestión del cambio (modelo ADKAR).

Entregable: Plan de despliegue y registro de capacitación.

Etapas 7. Operación y monitoreo

Durante la operación se monitorean KPIs técnicos y de SST, gestionando desviaciones y ajustando el sistema según resultados reales.

Entregable: Tablero de indicadores y registros de operación.

Etapas 8. Revisión y mejora continua

Se integran auditorías, revisión por la dirección y acciones de mejora, cerrando el ciclo PHVA aplicado a la IA.

Entregable: Informe de revisión y mejora.

Proceso de integración en ocho etapas: entradas, actividades y salidas.

Etapas	Entradas	Actividades clave	Salidas
1. Casos de uso	Problema; datos; objetivos	Identificar y priorizar	Catálogo de casos de uso
2. Contexto/stakeholders	Mapa de procesos; actores	Análisis de impacto y expectativas	Matriz de partes interesadas
3. EIIA	Datos; riesgos	Evaluar riesgos técnicos/éticos/psicosociales	Registro de riesgos y tratamiento
4. Diseño	Requisitos; políticas	Definir datos, desempeño, XAI, privacidad	Especificación técnica/funcional
5. V&V	Prototipos; criterios	Pruebas de laboratorio y campo	Informe V&V
6. Despliegue	Capacitación; plan	Implementación gradual; cambio	Plan de despliegue y capacitación
7. Operación	Tablero; SLAs	Monitoreo y respuesta	Registros y KPIs
8. Mejora	Lecciones; auditorías	Acciones correctivas y preventivas	Informe de mejora

7.4 Roles y responsabilidades

La integración de IA en SST requiere una clara definición de roles:

- Alta Dirección: patrocinio, aprobación de políticas y recursos.
- Profesional EHS: liderazgo preventivo, validación de casos de uso y métricas.
- Área TI / Datos: diseño técnico, seguridad y mantenimiento del sistema.
- Recursos Humanos: gestión del cambio y formación.
- Trabajadores y supervisores: retroalimentación y uso responsable del sistema.

Esta asignación favorece la rendición de cuentas y la sostenibilidad de la solución.

Tabla 6.2. Matriz RACI para la integración de IA en el SG-SST.

Actividad	Alta Dirección	EHS	TI/Datos	RR.HH.	Línea/Obra
Casos de uso	I	R	C	C	A
Gestión de riesgos de IA	I	A	R	C	I
Datos y privacidad	A	C	R	C	I
V&V y pilotos	I	R	R	I	A
Despliegue y cambio	I	A	R	R	A
Monitoreo y KPIs	I	A	R	I	R

7.5 Matriz de riesgos, controles y métricas

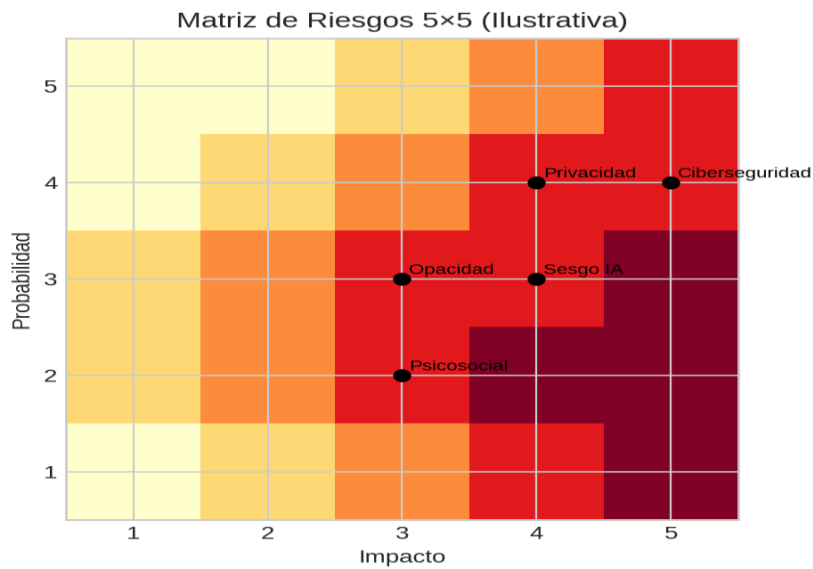
A partir del análisis realizado, se identifican riesgos críticos y controles asociados:

- Sesgo algorítmico: gobernanza de datos, validación periódica.
- Falta de explicabilidad: uso de modelos interpretables y documentación.
- Privacidad: minimización de datos, anonimización y control de accesos.
- Riesgos psicosociales: límites de monitoreo y participación de trabajadores.

- Ciberseguridad: gestión de vulnerabilidades y monitoreo continuo.

Cada riesgo debe vincularse a métricas verificables, integradas al sistema de seguimiento del SG-SST.

Matriz de riesgos 5x5 con ubicación de riesgos típicos de IA.



7.6 Indicadores clave de desempeño (KPI)

Se proponen indicadores en tres niveles:

1) Indicadores de SST:

- Tasa de accidentabilidad.
- Near-miss por horas trabajadas.
- Cumplimiento de EPP.

2) Indicadores técnicos:

- Precisión y sensibilidad del sistema de IA.
- Tasa de falsas alertas.
- Tiempo medio de respuesta (MTTR).

3) Indicadores sociotécnicos

- Aceptación de usuarios.
- Fatiga de alertas.
- Resultados de encuestas de clima y percepción.

Estos KPI permiten evaluar tanto el impacto preventivo como la sostenibilidad organizacional del sistema.

Indicadores clave de desempeño (definiciones, fuentes y umbrales de acción).

KPI	Definición operativa	Fórmula/Unidad	Fuente	Frecuencia	Umbral/Acción
Tasa de accidentabilidad (TRIR)	Incidentes por 200.000 h	Nº/200.000 h	Registros SST	Mensual	Revisión a +10%
Near-miss/10.000 h	Eventos sin lesión por 10.000 h	Nº/10.000 h	Reportes; PLN	Mensual	Investigación > 2σ
Cumplimiento de EPP (%)	% detecciones correctas de EPP	%	Visión IA	Semanal	Intervención < 85%
MTTR (min)	Tiempo medio de reacción a alertas	min	Tablero	Mensual	Escalar > SLA
Precisión/Sensibilidad	Desempeño del sistema IA	%	V&V	Mensual	Recalibrar < 0,85

7.7 Modelo de madurez para la integración de IA en SST

Se propone un modelo de madurez de cinco niveles:

- Inicial: uso experimental sin gobernanza formal.
- Repetible: casos de uso definidos y métricas básicas.
- Definido: gobernanza estructurada e integración con el SG-SST.
- Gestionado: desempeño medido y mejora basada en datos.
- Optimizado: IA integrada como capacidad estratégica preventiva.

Este modelo permite a la organización evaluar su progreso y definir hojas de ruta realistas.

Modelo de madurez para la integración de IA (niveles 1–5).

Nivel	Descripción	Enfoque SST/IA
1 – Inicial	Pilotos aislados, sin gobernanza	Métricas reactivas; riesgos no gestionados
2 – Repetible	Procesos básicos y catálogo de casos	Métricas por caso; documentación básica
3 – Definido	Gobernanza formal y roles claros	KPIs integrados al SG-SST; EIIA sistemática
4 – Gestionado	Mejora basada en datos y auditorías	Optimización de desempeño; cambio gestionado
5 – Optimizado	IA como capacidad estratégica	Prevención predictiva; aprendizaje continuo

7.8 Síntesis de la propuesta

La propuesta presentada integra la IA dentro del SG-SST de forma responsable, sistemática y alineada con estándares internacionales, asegurando que los beneficios preventivos se materialicen sin comprometer la seguridad, la salud ni los derechos de los trabajadores. Esta integración constituye la base para su aplicación práctica, desarrollada en el capítulo siguiente.

Capítulo 8. Caso práctico: integración de IA en obras menores de construcción (Chile)

8.1 Contexto y alcance del caso

El caso práctico se sitúa en el sector de obras menores de construcción en Chile, caracterizado por alta variabilidad de tareas, subcontratación y coexistencia de múltiples frentes de trabajo. Los peligros críticos priorizados son: caídas de altura, golpes por objetos y riesgos eléctricos, con conducta preventiva fuertemente vinculada al uso correcto de EPP y al respeto de zonas de exclusión (ISO, 2018; MINSAL, 1999/DS 594). La línea base considera: **(a)** tasa de accidentabilidad anual de la empresa y del sector (SUSESO, 2024); **(b)** near-miss/10.000 h y cumplimiento de EPP (%) de los últimos 6–12 meses; y **(c)** tiempos de reacción (MTTR) frente a observaciones críticas. La hipótesis operativa es que la incorporación gradual de visión por computador, PLN y un tablero de KPIs elevará el cumplimiento conductual y reducirá near-miss, con impacto medible en la frecuencia de incidentes (EU-OSHA, 2022; NIOSH, 2024).

Alcance. Tres frentes de obra activos durante 6–9 meses, con turnos diurnos, cuadrillas internas y contratistas. Los sistemas de IA se integran dentro del SG-SST (ISO 45001), bajo gobernanza de IA (NIST AI RMF; ISO/IEC 23894; ISO/IEC 42001) y resguardo de privacidad (Ley 19.628). (ISO, 2018; NIST, 2023; ISO/IEC, 2023a; ISO/IEC, 2023b; SUSESO, 2024).

8.2 Objetivos y metas del piloto

Objetivo general. Demostrar la viabilidad técnica y organizacional de integrar IA en el SG-SST para prevenir incidentes de alto impacto, resguardando derechos y aceptabilidad social.

Metas (12 meses, prudentes y defendibles)

- ↓ 20–30 % de incidentes registrables (TRIR/tasa de accidentabilidad) vs. línea base.
- ↓ 30–40 % de near-miss/10.000 h en 6–9 meses.
- ≥ 90 % de cumplimiento de EPP sostenido por frente.
- ↓ ≥ 20 % en MTTR ante alertas críticas.

(Metas alineadas con evidencia de reducciones observadas en analítica y visión por computador en contextos industriales comparables: EU-OSHA, 2022; NIOSH, 2024).

Línea base (ejemplo) y metas del piloto. Nota: datos sintéticos con fines ilustrativos.

Indicador	Línea base (ejemplo)	Meta 12 meses	Comentario
TRIR/tasa accidentabilidad	3,2 por 200.000 h	≤ 2,2	Meta prudente (-30%)
Near-miss/10.000 h	12,0	≤ 8,0	Reducción 30–40%
Cumplimiento EPP (%)	78%	≥ 90%	Sostenido 3 meses
MTTR (min)	45	≤ 36	-20% o más

8.3 Diseño metodológico del caso (cuasi-experimental)

Diseño A/B paralelo o serie temporal interrumpida (según disponibilidad):

- Grupo intervención (A): frentes 1–2 con visión por computador (EPP, intrusiones, posturas) + PLN (minería de reportes) + tablero de KPIs.
- Grupo control (B): frente 3 con prácticas estándar SG-SST sin IA.

Duración: 6–9 meses (fase piloto), con revisión a 12 meses.

Variables dependientes: near-miss/10.000 h; TRIR/tasa de accidentabilidad; cumplimiento EPP (%); MTTR (min); aceptación (encuestas).

Medición: semanal (cumplimiento EPP); mensual (near-miss, MTTR, aceptación); trimestral (accidentabilidad).

Análisis: comparación A vs. B y tendencias pre-pos; significancia ($p < 0,05$) cuando el tamaño muestral lo permita; énfasis en efecto práctico y consistencia de señales.

(ISO, 2018; NIST, 2023; ISO/IEC, 2023a; EU-OSHA, 2022).

Criterios de éxito (V&V operativa):

- Sensibilidad y precisión del sistema de visión $\geq$ umbrales definidos en pruebas de campo (p.ej., $\geq 0,85$ / $0,90$ para EPP).
- Falsa alarma en rango operativo aceptable (p.ej., $FPR < 10\%$; se ajusta por umbral).
- Utilidad percibida $\geq 75\%$ en supervisores (encuesta).
- No evidencia de daño psicosocial (encuesta clima/estrés estable).

(NIST, 2023; NIOSH, 2024).

8.4 Componentes tecnológicos y flujo de datos

- a) Visión por computador: cámaras en puntos críticos (accesos, zonas de altura, bodegas).
Detecciones: EPP (casco, chaleco, protección ocular), intrusiones en zonas de exclusión y posturas riesgosas seleccionadas.
- b) PLN: clasificación de reportes y observaciones (propios y de contratistas), estandarizando taxonomía de eventos y hallazgos.
- c) Tablero de KPIs: visualización near-miss, cumplimiento EPP, MTTR, tasa de incidentes; filtros por frente/contratista/semana.
- d) Controles: minimización de datos, anonimización/enmascaramiento cuando sea viable, acceso por rol, retención limitada y registro de decisiones (quién/qué/cuándo/por qué).
- e) Flujo: Captura $\rightarrow$ Ingesta/QA $\rightarrow$ Modelo IA (XAI + monitoreo de drift) $\rightarrow$ Alertas/Tablero $\rightarrow$ Respuesta en terreno $\rightarrow$ Registro y retroalimentación al modelo. (NIST, 2023; ISO/IEC, 2023b; Ley 19.628).

8.5 Gestión de riesgos, privacidad y relaciones laborales

Privacidad y datos personales (Ley 19.628): uso limitado al propósito preventivo, proporcionalidad, minimización, retención definida (p.ej., 30–90 días para video analítico), acceso por rol, y registro de incidentes de privacidad.

Riesgos psicosociales: prohibición explícita de uso disciplinario automático; participación temprana de trabajadores y comités paritarios; comunicación clara de objetivos y límites del monitoreo; encuestas de clima.

Sesgos/explicabilidad: datos de entrenamiento representativos (iluminación, ángulos, EPP local); documentación de decisiones y XAI para revisión de alertas.

Ciberseguridad: hardening de sistemas, parches, gestión de vulnerabilidades y pruebas periódicas.

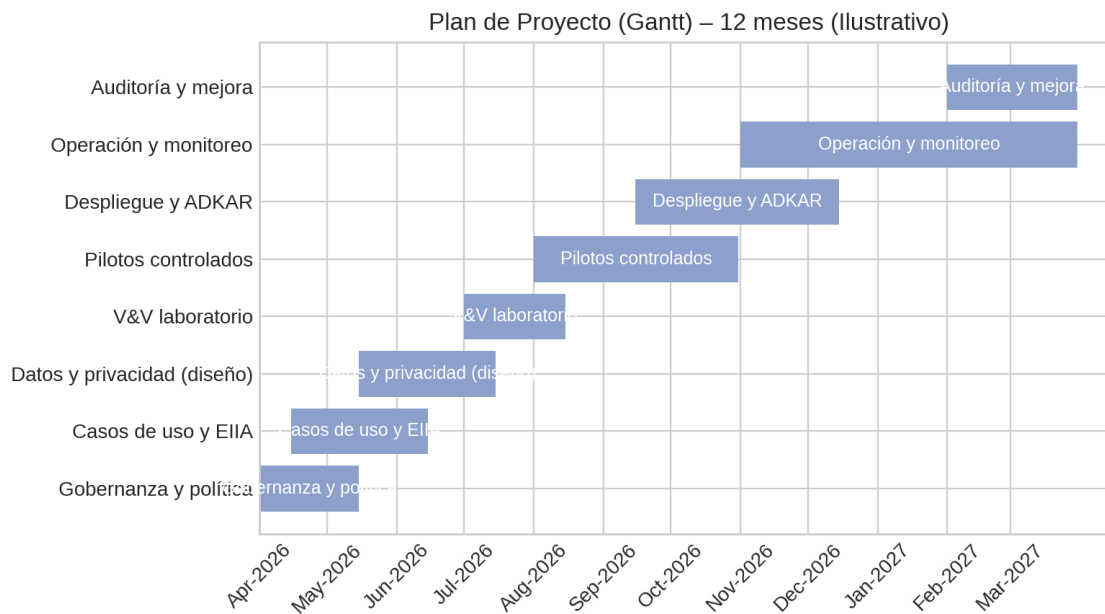
(OCDE, 2019; OIT, 2024; NIST, 2023; ISO/IEC, 2023a).

8.6 Plan de implementación (12 meses) y gestión del cambio

Fases y entregables principales

- Meses 1–2 | Gobernanza: política de IA en SST; inventario de casos de uso; EIIA inicial; RACI; plan de comunicaciones.
- Meses 2–3 | Datos y diseño: requisitos de datos, especificación (desempeño, XAI, seguridad, privacidad); criterios de aceptación.
- Meses 3–4 | V&V laboratorio: calibración y pruebas internas; protocolo de campo.
- Meses 5–7 | Piloto controlado: despliegue progresivo; capacitación; ajuste de umbrales; tablero operativo.
- Meses 8–9 | Evaluación: métricas técnicas y de SST; encuestas de aceptación/fatiga; informe intermedio.
- Meses 10–12 | Escalado y mejora: lecciones aprendidas; ajustes de procesos; revisión por la dirección.

Plan de implementación tipo Gantt (12 meses, ilustrativo).



Gestión del cambio (ADKAR):

Conciencia → Deseo → Conocimiento → Habilidad → Refuerzo. Acciones: talleres breves con supervisores, cápsulas de microaprendizaje, reconocimiento de buenas prácticas y retroalimentación visible en el tablero. (ISO, 2018; NIST, 2023).

8.7 Indicadores y tablero (definiciones operacionales)

a) Indicadores de SST

- Tasa de accidentabilidad (TRIR) = (incidentes registrables / 200.000 h).
- Near-miss/10.000 h (tasa).
- Cumplimiento EPP (%): detecciones correctas / total observaciones válidas.
- MTTR (min): tiempo desde alerta válida hasta acción registrada.

b) Indicadores técnicos

- Precisión / Sensibilidad de detecciones (visión).

- FPR/FNR (falsos positivos/negativos).
- Drift de datos/modelo (alertas de deriva).

c) Indicadores sociotécnicos

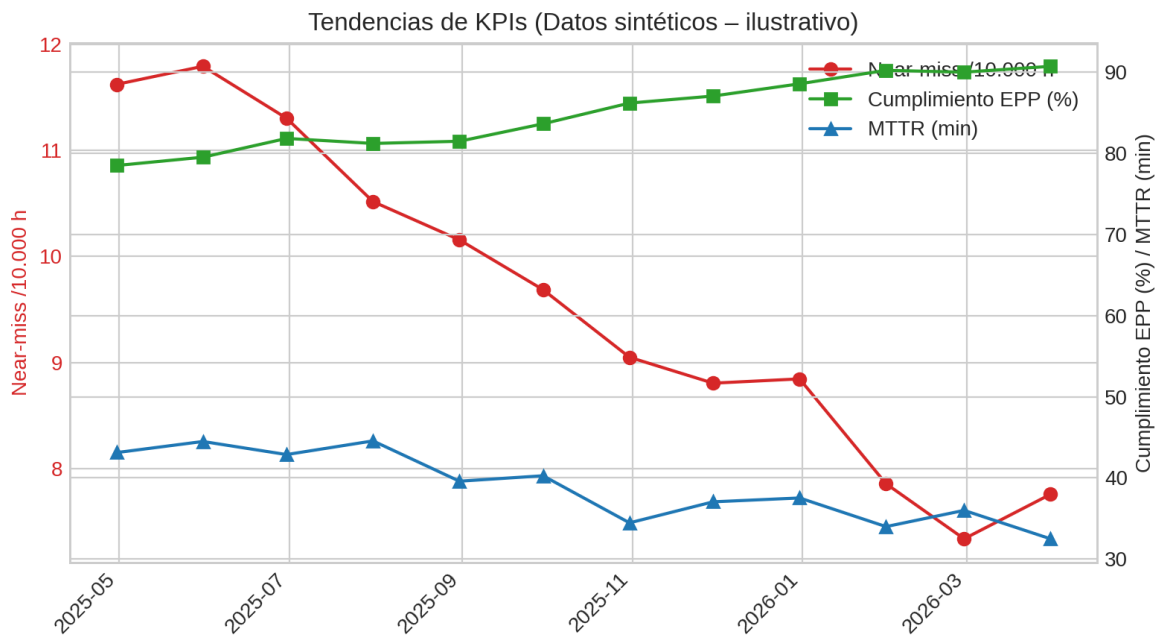
- Utilidad percibida; fatiga de alertas; clima/estrés (encuestas).

(NIST, 2023; NIOSH, 2024).

d) Reglas de acción ejemplo

- Cumplimiento EPP < 85 % por 2 semanas → intervención focalizada.
- MTTR > SLA (p.ej., 10 min) → escalamiento a jefatura.
- FPR > 15 % → recalibración de umbrales y revisión de cámaras/iluminación.

Tendencias de KPIs (near-miss, cumplimiento EPP, MTTR). Nota: datos sintéticos para ilustración.



8.8 Evaluación de impacto y análisis económico

Evaluación de impacto

- Comparación A/B de tasas (near-miss, EPP, MTTR, TRIR).
- Intervalos de confianza y pruebas de significancia cuando aplique (tamaño muestral suficiente).
- Triangulación con auditorías de campo y entrevistas a supervisores.

Análisis costo–beneficio (orientativo)

- CAPEX: cámaras (si no existen), licencias/piloto, configuración.
- OPEX: soporte, mantenimiento, almacenamiento, capacitación.
- Beneficios: reducción de incidentes/ausentismo, tiempo de supervisión, multas/retrabajos, reputación y continuidad operacional.
- (ISO, 2018; EU-OSHA, 2022; SUSESO, 2024).

8.9 Resultados esperados y criterios de cierre

Se espera confirmar:

- Mejora sostenida de cumplimiento EPP y reducción de near-miss;
- Disminución de MTTR y mejora en la priorización de controles;
- Aceptación ≥ 75 % en usuarios clave;
- Cero incidentes de privacidad;
- Evidencias suficientes para escalar o ajustar la solución.

Criterios de cierre: informe técnico con métricas consolidadas, lecciones aprendidas, actualizaciones de procedimientos y revisión por la dirección con decisión de continuidad/escalado.

8.10 Riesgos residuales y planes de contingencia

Cambios de iluminación → recalibración periódica; viseras/zonas sombreadas; pruebas por turno.

Resistencia de usuarios → reforzar comunicaciones, límites de uso y beneficios; incluir champions de cuadrilla.

Datos incompletos → normalizar taxonomías; mejorar disciplina de reporte; QA de datos.

Sobrecarga de alertas → umbrales adaptativos; agrupamiento; revisión humana.

Ciberseguridad → pruebas de penetración y monitoreo de vulnerabilidades.

(NIST, 2023; ISO/IEC, 2023a; OIT, 2024).

8.11 Síntesis del caso

El caso práctico demuestra una ruta realista y auditable para integrar IA en obras menores de construcción, respetando el SG-SST y la legislación chilena. La propuesta equilibra valor preventivo con privacidad, aceptación y gobernanza, permitiendo sostener resultados y escalar bajo un modelo de madurez medible.

Capítulo 9. Conclusiones y líneas futuras

9.1 Síntesis de hallazgos

Este Trabajo Fin de Máster demostró que la integración de la inteligencia artificial (IA) al Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) es viable, útil y auditable cuando se gobierna bajo estándares internacionales y se implementa con participación efectiva de las personas. Desde el análisis teórico y normativo hasta el caso práctico en obras menores de construcción (Chile), los resultados convergen en tres ideas fuerza:

- Valor preventivo medible. La IA —especialmente visión por computador (EPP, intrusiones, posturas) y analítica/PLN (minería de reportes)— permite anticipar riesgos, priorizar controles y reducir la dependencia de inspecciones puntuales. El valor emerge cuando estas tecnologías se

insertan en los procesos del SG-SST con metas, umbrales y responsabilidades claras (ISO, 2018; NIOSH, 2024).

- Riesgos gestionables con gobernanza. Sesgos, opacidad, privacidad, ciberseguridad y efectos psicosociales no invalidan el uso de IA, pero exigen gestión de riesgos específica (NIST AI RMF; ISO/IEC 23894) y un sistema de gestión de IA (ISO/IEC 42001) que asegure trazabilidad, explicabilidad proporcional y controles organizacionales (NIST, 2023; ISO/IEC, 2023a, 2023b).
- Compatibilidad estructural con ISO 45001. Existe trazabilidad robusta entre liderazgo-participación ↔ GOVERN (NIST), planificación ↔ MAP/23894, operación ↔ MANAGE/42001, evaluación ↔ MEASURE y mejora ↔ ciclo PHVA, lo que permite auditorías integradas y evita proyectos tecnológicos “en paralelo” (ISO, 2018; NIST, 2023).

9.2 Conclusiones principales

C1. La IA agrega capacidad preventiva al SG-SST cuando se diseña como apoyo a la decisión y no como sustituto del criterio profesional; su impacto positivo depende de datos de calidad, validación en campo y diseño centrado en las personas (EU-OSHA, 2022; ISO, 2018).

C2. La gobernanza es condición habilitante: políticas, roles (RACI), Evaluación de Impacto de IA (EIIA), V&V, métricas y auditorías inspiran confianza, reducen riesgos y convierten la IA en capacidad organizacional (NIST, 2023; ISO/IEC, 2023b).

C3. El caso práctico muestra una ruta realista para despliegue: pilotos graduales, ADKAR para gestión del cambio, tablero de KPI y reglas de acción. Los criterios de éxito combinan métricas de SST (near-miss, EPP, MTTR, accidentabilidad) con métricas técnicas y sociotécnicas (precisión/sensibilidad, FPR/FNR, aceptación, fatiga de alertas).

C4. La aceptación depende de límites y propósito: privacidad por diseño, participación de trabajadores/comités paritarios y prohibición del uso disciplinario automático preservan el enfoque de trabajo decente (OIT, 2024; Ley 19.628).

9.3 Recomendaciones prácticas para la implantación

- a) Definir una Política de IA en SST aprobada por la alta dirección (propósito, principios, límites, métricas y auditoría).
- b) Inventariar casos de uso y priorizar por valor preventivo y criticidad (matriz beneficio-riesgo).
- c) Aplicar EIIA antes de cada piloto (técnica, ética, psicosocial y privacidad), según ISO/IEC 23894 y NIST AI RMF.
- d) Diseñar requisitos de datos (calidad, linaje, minimización, retención/borrado, acceso por rol) y de explicabilidad proporcional al riesgo.
- e) Verificar y validar (V&V) en laboratorio y campo con criterios de aceptación (precisión, sensibilidad, FPR/FNR, utilidad percibida).
- f) Desplegar gradualmente con ADKAR (conciencia-deseo-conocimiento-habilidad-refuerzo) y capacitación práctica para supervisores/cuadrillas.
- g) Monitorear con KPI integrados al SG-SST (SST + técnicos + sociotécnicos), tablero y reglas de acción (umbral → respuesta → aprendizaje).
- h) Auditar y mejorar con la doble perspectiva 45001–42001: hallazgos, acciones correctivas y revisión por la dirección.

9.4 Implicancias para el rol del profesional EHS

El profesional de EHS se posiciona como traductor sociotécnico: conecta riesgos “duros” de operación con riesgos de IA y factores humanos, lidera la gestión del cambio y vela por que las métricas sirvan a la prevención, no a la vigilancia. Sus competencias clave incluyen criterio técnico, alfabetización en datos/IA, ética, privacidad y comunicación (NIOSH, 2024; OIT, 2024).

9.5 Limitaciones del estudio

Datos empíricos: el TFM se apoya en literatura y marcos 2018–2026 y en un diseño de caso; las series reales (KPIs) deben incorporarse en la implementación para confirmar magnitudes.

Generalización contextual: la propuesta se ajusta a obras menores y marco chileno; su extrapolación a otros sectores/países exige adaptación normativa y organizacional.

Tecnologías específicas: no se comparan proveedores; los resultados dependen de calidad de datos, condiciones ambientales y disciplina de uso en obra.

9.6 Líneas futuras de trabajo

- a) Gemelos digitales y simulación de escenarios para planificar controles, gestionar congestiones y ensayar emergencias con integración EHS-IA.
- b) IA generativa para formación (micro-simulaciones, briefing de riesgo, análisis causal asistido), respetando privacidad y sesgos.
- c) Monitoreo de drift de datos/modelos y MLOps seguro (ciclo de vida, parches, gestión de vulnerabilidades) integrado al SG-SST.
- d) Evaluación de impacto psicosocial longitudinal (aceptación, confianza, carga mental y fatiga de alertas) y co-diseño con trabajadores.
- e) Integración con SGSI/privacidad (ISO/IEC 27001, 27701) para reforzar ciberseguridad y cumplimiento de datos personales.
- f) Economía de la prevención: modelos de costo-beneficio con datos reales (CAPEX/OPEX vs. ahorros por accidentes evitados y continuidad operacional).

9.7 Cierre y aportes

La IA no es un fin en sí misma, sino una capacidad preventiva cuando se diseña con personas, procesos y evidencia en el centro. Un SG-SST que integra IA con gobernanza, métricas y participación no solo reduce riesgos: aprende más rápido, decide mejor y construye una cultura preventiva resiliente.

9.7.1 Aportes del TFM

Guía operativa con evidencias auditables: inventario de casos de uso, Evaluación de Impacto de IA (EIIA), protocolos de verificación y validación, tablero de KPI, registros de decisiones y matriz de riesgos.

Trazabilidad ISO 45001 ↔ NIST AI RMF/ISO-IA, habilitando auditorías integradas y cruzadas.

Modelo de madurez y procedimiento (SOP) de integración IA–SST para gestión del cambio (ADKAR), datos (calidad, minimización y retención) y privacidad por diseño.

Caso práctico contextualizado a Chile (obras menores), con metas prudentes y diseño de evaluación.

Capítulo 10. Anexos

Introducción a los Anexos

Los anexos que se presentan a continuación constituyen un complemento operativo y metodológico del Trabajo Fin de Máster, cuyo propósito es respaldar, ampliar y operacionalizar los contenidos desarrollados en los capítulos principales. Mientras el cuerpo del trabajo aborda el análisis conceptual, normativo y aplicado de la integración de la inteligencia artificial (IA) en los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST), los anexos proporcionan herramientas prácticas, formatos y procedimientos que permiten materializar dicha integración en contextos organizacionales reales.

En particular, los anexos incluyen políticas, procedimientos, matrices, plantillas y formatos diseñados para ser auditables, replicables y coherentes con los requisitos de ISO 45001, así como con los marcos internacionales de gobernanza y gestión de riesgos de la IA, tales como el NIST AI Risk Management Framework, la ISO/IEC 23894 y la ISO/IEC 42001. Su incorporación responde a la necesidad de demostrar que la propuesta desarrollada no se limita a un enfoque teórico, sino que puede ser implementada de forma estructurada, respetando principios de prevención, participación de los trabajadores, protección de datos personales y mejora continua.

Asimismo, estos anexos cumplen una función clave desde la perspectiva académica y profesional, ya que evidencian la viabilidad operativa de la propuesta, facilitan su evaluación por parte del tribunal y aportan valor añadido al profesional de EHS que busque aplicar la inteligencia artificial como herramienta de apoyo a la gestión preventiva. Cada anexo ha sido elaborado para integrarse de manera directa al SG-SST de una organización, sirviendo como base para políticas internas, procedimientos operativos estándar, evaluaciones de impacto, seguimiento de indicadores y procesos de toma de decisiones informadas.

En conjunto, los anexos refuerzan el carácter aplicado, sistemático y orientado a la práctica del presente Trabajo Fin de Máster, consolidando la propuesta de integración de la inteligencia artificial en la gestión de la seguridad y salud en el trabajo como una alternativa responsable, medible y alineada con estándares internacionales.

Anexo A. Política de Inteligencia Artificial en Seguridad y Salud en el Trabajo

A.1 Propósito

Establecer los principios, responsabilidades y lineamientos para el diseño, adquisición, implementación y operación de sistemas de inteligencia artificial (IA) aplicados a la Seguridad y Salud en el Trabajo (SST), asegurando la protección de la seguridad, salud, derechos fundamentales y privacidad de los trabajadores.

A.2 Alcance

Esta política aplica a todos los sistemas de IA utilizados con fines preventivos en SST, incluyendo visión por computador, analítica predictiva y procesamiento de lenguaje natural, tanto en personal propio como contratistas.

A.3 Principios

- IA como apoyo a la prevención, no sustituto del criterio profesional.
- Centralidad de las personas y enfoque de trabajo decente.
- Proporcionalidad según criticidad del riesgo.
- Transparencia y explicabilidad de las decisiones.
- Privacidad y protección de datos por diseño.
- Participación de trabajadores y mejora continua.

A.4 Responsabilidades

- Alta Dirección: aprobación de la política y provisión de recursos.
- EHS: validación preventiva de casos de uso y métricas.
- TI/Datos: seguridad, desempeño y mantenimiento.
- RR.HH.: gestión del cambio y formación.

A.5 Revisión

La política será revisada anualmente o ante cambios significativos en la tecnología o la normativa.

Anexo B. Procedimiento Operativo Estándar (SOP) – Integración de IA en el SG-SST

B.1 Objetivo

Definir el procedimiento para integrar IA en el SG-SST de manera sistemática y auditable.

B.2 Procedimiento resumido

- Identificación y priorización de casos de uso.
- Análisis de contexto y partes interesadas.
- Evaluación de Impacto de IA (EIIA).
- Diseño de requisitos técnicos y organizacionales.
- Verificación y validación (V&V).
- Despliegue controlado y capacitación.
- Operación y monitoreo.
- Revisión y mejora continua.

B.3 Registros asociados

- Inventario de sistemas de IA.
- Registro de riesgos de IA.
- Informes de V&V.
- Tablero de KPIs.
- Actas de revisión por la dirección.

Anexo C. Plantilla de Evaluación de Impacto de IA (EIIA)

C.1 Identificación del sistema

- Nombre del sistema:
- Caso de uso:
- Responsable:

C.2 Objetivo preventivo

- Riesgos de SST abordados:
- Valor preventivo esperado:

C.3 Datos y privacidad

- Tipo de datos tratados:
- Datos personales involucrados: Sí / No
- Medidas de minimización y anonimización:

C.4 Riesgos identificados

- Técnicos (sesgos, errores, fallos):
- Organizacionales:
- Psicosociales:

C.5 Controles y métricas

- Controles técnicos:
- Controles organizacionales:
- KPIs asociados:

C.6 Conclusión

- Riesgo residual aceptable: Sí / No
- Recomendaciones:

Anexo D. Matriz de riesgos de IA aplicada a SST (ISO/IEC 23894)

Riesgo	Impacto	Probabilidad	Control	KPI
Sesgo algorítmico	Alto	Medio	Gobernanza de datos	Δ disparidad
Falta de explicabilidad	Medio	Medio	XAI y trazabilidad	% decisiones explicadas
Privacidad	Alto	Bajo	Minimización y acceso por rol	Incidentes
Fatiga de alertas	Medio	Medio	Umbrales adaptativos	Alertas/turno
Ciberseguridad	Alto	Bajo	Hardening y parches	MTTR ciber

Anexo E. Indicadores clave de desempeño (KPIs) y tablero

E.1 KPIs de SST

- Tasa de accidentabilidad (TRIR).
- Near-miss por 10.000 horas.
- Cumplimiento de EPP (%).

E.2 KPIs técnicos

- Precisión y sensibilidad del sistema.
- Tasa de falsas alertas.
- Drift de datos/modelo.

E.3 KPIs sociotécnicos

- Aceptación de usuarios (%).
- Fatiga de alertas.
- Resultados de encuestas de clima.

Anexo F. Checklist de evaluación de proveedores de IA

- Evidencia de desempeño en campo.
- Mecanismos de explicabilidad (XAI).
- Cumplimiento de privacidad y seguridad.
- Documentación técnica y soporte.
- Compatibilidad con ISO 45001 / 42001.
- Condiciones de escalabilidad y costos.

Anexo G. Modelo de consentimiento informado para trabajadores

G.1 Propósito del sistema

Uso de IA con fines **exclusivamente preventivos** en SST.

G.2 Tipo de datos tratados

Imágenes/video analítico, reportes de seguridad, métricas agregadas.

G.3 Derechos del trabajador

- Información clara sobre el sistema.
- Acceso, rectificación y consulta.
- Canales de reclamo.

G.4 Declaración El trabajador declara haber sido informado del propósito, alcance y límites del sistema de IA.

Firma:

Fecha: _____

Conclusión de los Anexos

Los anexos presentados en este Trabajo Fin de Máster constituyen un soporte fundamental para la implementación práctica de la propuesta de integración de la inteligencia artificial (IA) en los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST). Su desarrollo responde a la necesidad de trasladar los principios conceptuales y normativos expuestos en el cuerpo del documento a instrumentos operativos concretos, facilitando su aplicación en entornos organizacionales reales.

A través de políticas, procedimientos, matrices, plantillas e indicadores, los anexos permiten operacionalizar la gobernanza de la IA en SST, asegurando coherencia con los requisitos de ISO 45001, así como con los marcos internacionales de gestión de riesgos y sistemas de gestión de IA. De este modo, se refuerza la trazabilidad entre la identificación de peligros, la evaluación de riesgos, la toma de decisiones apoyada por IA y la mejora continua del desempeño preventivo.

Asimismo, los anexos aportan valor desde una perspectiva académica y profesional, al evidenciar que la propuesta desarrollada es replicable, auditable y adaptable a distintos contextos organizacionales, particularmente en sectores de alta variabilidad operativa como la construcción. Su utilización permite al profesional de EHS contar con herramientas estructuradas para gestionar los riesgos asociados a la IA, promover la participación de los trabajadores, resguardar la privacidad y medir de manera objetiva el impacto de estas tecnologías en la prevención de accidentes y enfermedades profesionales.

En conjunto, los anexos consolidan el carácter aplicado, sistemático y orientado a la mejora continua del presente TFM, reforzando la viabilidad de la inteligencia artificial como una herramienta estratégica de apoyo a la gestión preventiva, siempre que su integración se realice bajo principios de responsabilidad, transparencia y alineación con estándares internacionales.

Recomendaciones finales

A partir del análisis teórico, normativo y aplicado desarrollado en este Trabajo Fin de Máster, se proponen las siguientes recomendaciones finales, orientadas a favorecer una integración efectiva, responsable y sostenible de la inteligencia artificial (IA) en los Sistemas de Gestión de Seguridad y Salud en el Trabajo (SG-SST).

1. Integrar la IA como parte del sistema de gestión, no como solución aislada

Las organizaciones deben evitar implementar la inteligencia artificial como un proyecto tecnológico independiente. En su lugar, se recomienda integrarla explícitamente dentro del SG-SST basado en ISO

45001, alineando los casos de uso de IA con los procesos existentes de identificación de peligros, evaluación de riesgos, control operacional, seguimiento del desempeño y mejora continua. Esta integración sistémica es clave para asegurar coherencia, trazabilidad y sostenibilidad en el tiempo.

2. Establecer una gobernanza clara de la IA aplicada a SST

Se recomienda definir una estructura de gobernanza de IA, con políticas, roles y responsabilidades claramente asignados. La adopción de marcos como el NIST AI Risk Management Framework, junto con estándares como ISO/IEC 23894 e ISO/IEC 42001, permite gestionar de manera estructurada los riesgos técnicos, organizacionales y humanos asociados a la IA, reforzando la rendición de cuentas y la confianza de las partes interesadas.

3. Priorizar casos de uso con alto valor preventivo y bajo impacto negativo

No todos los usos de la IA aportan el mismo valor en términos de prevención. Se recomienda priorizar aquellos casos de uso que presenten un alto impacto preventivo, como la verificación de EPP, la detección de condiciones críticas o el análisis de near-miss, y que, al mismo tiempo, impliquen menores riesgos de privacidad o efectos psicosociales. Esta priorización favorece una adopción gradual y socialmente aceptable.

4. Incorporar la Evaluación de Impacto de IA como práctica estándar

Antes de implementar cualquier sistema de IA en SST, se recomienda realizar una Evaluación de Impacto de IA (EIIA) que considere no solo aspectos técnicos, sino también éticos, psicosociales y legales. Esta práctica permite anticipar riesgos, definir controles proporcionales y documentar decisiones, alineándose con el principio preventivo propio de la SST y con las exigencias de protección de datos personales.

5. Asegurar la participación y comunicación con los trabajadores

La aceptación de la IA en entornos laborales depende en gran medida de la participación temprana y efectiva de los trabajadores. Se recomienda involucrar a supervisores, cuadrillas y comités paritarios desde las etapas iniciales de diseño e implementación, comunicando de forma clara el propósito preventivo, los límites de uso y las garantías de privacidad. Esta participación contribuye a reducir resistencias y riesgos psicosociales.

6. Definir y monitorear indicadores técnicos y preventivos relevante

La implementación de IA en SST debe estar acompañada de indicadores clave de desempeño (KPI) que permitan evaluar su efectividad real. Se recomienda combinar indicadores de resultados en SST (accidentabilidad, near-miss, cumplimiento de EPP) con indicadores técnicos (precisión, sensibilidad, falsas alertas) y sociotécnicos (aceptación de usuarios, fatiga de alertas). Este enfoque integral facilita la toma de decisiones basada en evidencia.

7. Fortalecer el rol del profesional EHS frente a la transformación digital

La integración de la IA exige que el profesional de EHS desarrolle competencias adicionales en gestión de datos, comprensión básica de IA, ética y factores humanos. Se recomienda promover programas de formación que fortalezcan este rol como articulador entre tecnología y prevención, asegurando que las decisiones apoyadas por IA mantengan siempre un enfoque humano y preventivo.

8. Promover la mejora continua y el aprendizaje organizacional

Finalmente, se recomienda utilizar la IA como una herramienta para potenciar el aprendizaje organizacional, integrando los resultados obtenidos en la revisión periódica del SG-SST. La revisión por la dirección, las auditorías internas y el análisis de datos generados por los sistemas de IA deben alimentar un ciclo permanente de mejora, coherente con el enfoque PHVA y con una cultura preventiva madura.

Capítulo 11. Referencias

Referencias citadas en capítulo 1 (formato APA)

European Agency for Safety and Health at Work. (2022). Artificial intelligence and occupational safety and health: Discussion paper. Author.

International Labour Organization. (2024). Global strategy on occupational safety and health 2024–2030. Author.

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Risk management. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023b). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. Author.

National Institute for Occupational Safety and Health. (2024). Considerations for the use of AI in occupational safety and health. Author.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.

Organisation for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence. Author.

Referencias del Capítulo 2 (APA 7)

European Agency for Safety and Health at Work. (2022). Artificial intelligence and occupational safety and health: Discussion paper. Author.

International Labour Organization. (2024). Global strategy on occupational safety and health 2024–2030. Author.

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Risk management. Author.

National Institute for Occupational Safety and Health. (2024). Considerations for the use of AI in occupational safety and health. Author.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.

Referencias del Capítulo 3 (APA 7)

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Risk management. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023b). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. Author.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.

Organisation for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence. Author.

Organización Internacional del Trabajo. (2024). Estrategia global de seguridad y salud en el trabajo 2024-2030. OIT.

Ministerio de Salud de Chile. (1999). Decreto Supremo N° 594.

Superintendencia de Seguridad Social. (2024). Estadísticas de accidentabilidad laboral.

Referencias del Capítulo 4 (APA 7)

European Agency for Safety and Health at Work. (2022). Artificial intelligence and occupational safety and health: Discussion paper. Author.

International Labour Organization. (2024). Global strategy on occupational safety and health 2024-2030. Author.

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.

Organisation for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence. Author.

Referencias del Capítulo 5 (APA 7)

European Agency for Safety and Health at Work. (2022). Artificial intelligence and occupational safety and health: Discussion paper. Author.

International Labour Organization. (2024). Global strategy on occupational safety and health 2024-2030. Author.

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Risk management. Author.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.

National Institute for Occupational Safety and Health. (2024). Considerations for the use of AI in occupational safety and health. Author.

Referencias del Capítulo 6 (APA 7)

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Risk management. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023b). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. Author.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.

Organisation for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence. Author.

Referencias del Capítulo 7 (APA 7)

European Agency for Safety and Health at Work. (2022). Artificial intelligence and occupational safety and health: Discussion paper. Author.

International Labour Organization. (2024). Global strategy on occupational safety and health 2024–2030. Author.

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Risk management. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023b). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. Author.

Ministerio de Salud de Chile. (1999). Decreto Supremo N° 594: Reglamento sobre condiciones sanitarias y ambientales básicas.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.

National Institute for Occupational Safety and Health. (2024). Considerations for the use of AI in occupational safety and health. Author.

Superintendencia de Seguridad Social. (2024). Estadísticas de accidentabilidad laboral.

Organización de Cooperación y Desarrollo Económicos. (2019). Principios de IA. OCDE.

Referencias del Capítulo 8 (APA 7)

European Agency for Safety and Health at Work. (2022). Artificial intelligence and occupational safety and health: Discussion paper. Author.

International Labour Organization. (2024). Global strategy on occupational safety and health 2024–2030. Author.

International Organization for Standardization. (2018). ISO 45001:2018 Occupational health and safety management systems—Requirements with guidance for use. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Risk management. Author.

International Organization for Standardization & International Electrotechnical Commission. (2023b). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. Author.

National Institute for Occupational Safety and Health. (2024). Considerations for the use of AI in occupational safety and health. Author.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Author.