OM EDITORIAL

TRANSFORMACIÓN DIGITAL Y ANALÍTICA DE DATOS PARA LA PREVENCIÓN DE RIESGOS

Inteligencia Artificial, Big Data e Innovación en la Gestión de la Seguridad y Salud

Chang-Gómez, Mario Andrew; Malca-Salas, Gustavo Adolfo; Souza-Najar, Rosa Isabel; Araujo-Dávila, Carlos Enrique; Wong-Ramírez, Jandira del Pilar; Vásquez-Pinedo, Jorge Armando; Casas-Tello, Dan Elias; Ramírez-Álvarez, Karenth Elena; Vásquez-Gil, Oscar Alberto; Carrasco-Montañez, Daniel Diomedes

Transformación Digital y Analítica de Datos para la Prevención de Riesgos:

Inteligencia Artificial, Big Data e Innovación en la Gestión de la Seguridad y Salud.

Autor/es:

Chang-Gómez, Mario Andrew
Universidad Nacional de la Amazonía Peruana

Malca-Salas, Gustavo Adolfo
Universidad Nacional de la Amazonía Peruana

Souza-Najar, Rosa Isabel
Universidad Nacional de la Amazonía Peruana

Araujo-Dávila, Carlos Enrique
Universidad Nacional de la Amazonía Peruana

Wong-Ramírez, Jandira del Pilar
Universidad Nacional de la Amazonía Peruana

Vásquez-Pinedo, Jorge Armando
Universidad Nacional de la Amazonía Peruana

Casas-Tello, Dan Elias
Universidad Nacional de la Amazonía Peruana

Ramírez-Álvarez, Karenth Elena
Universidad Nacional de la Amazonía Peruana

Vásquez-Gil, Oscar Alberto
Universidad Nacional de la Amazonía Peruana

Carrasco-Montañez, Daniel Diomedes
Universidad Nacional de la Amazonía Peruana

Datos de Catalogación Bibliográfica

Chang-Gomez, M. A.
Malca-Salas, G. A.
Souza-Najar, R. I.
Araujo-Dávila, C. E.
Wong-Ramirez, J. P.
Vasquez-Pinedo, J. A.
Casas-Tello, D. E.
Ramírez-Álvarez, K.E.
Vásquez-Gil, O. A.
Carrasco-Montañez, D. D.

Transformación Digital y Analítica de Datos para la Prevención de Riesgos
Oriente-Manabí Editorial, Ecuador, 2026
ISBN: 978-9907-9567-5-7
Formato: 210 mm X 270 mm 104 págs.

Publicado por Oriente-Manabí Editorial
Ecuador, Manabí, Cod. Post. 130101.
Contacto: +593 959 723 343
Email: info@omeditorial.com
www.books.omeditorial.com

Director General:	*Dr. Guerrero Bermúdez Ángel Enrique*
Editor en Jefe:	*Dr. Guerrero Bermúdez Ángel Enrique*
Editor Académica:	*Lcdo. Oltramonti Roberto, Mg*
Supervisor de Producción:	*Ing. Barragán Monrroy Roberto Johan, Mg.*
Diseño:	*OM Editorial*
Consejo Editorial	*OM Editorial*

Libro Digital, Primera Edición, 2026
Editado, Diseñado, Diagramado y Publicado por Comité OM Editorial
Manabí, Ecuador, 2026

Cámara Ecuatoriana del Libro con Radicación editorial 182865

Título del libro:
Transformación Digital y Analítica de Datos para la Prevención de Riesgos: Inteligencia Artificial, Big Data e Innovación en la Gestión de la Seguridad y Salud.

ISBN: 978-9907-9567-5-7

https://doi.org/10.63618/omeditorial/l30

Como citar (APA 7ma Edición):
Chang-Gómez, M. A., Vásquez-Gil, O. A., Ramírez-Álvarez, K. E., Casas-Tello, D. E., Vasquez-Pinedo, J. A., Wong-Ramirez, J. del P., Araujo-Dávila, C. E., Souza-Najar, R. I., Malca-Salas, G. A., & Carrasco-Montañez, D. D. (n.d.). *Transformación Digital y Analítica de Datos para la Prevención de Riesgos: Inteligencia Artificial, Big Data e Innovación en la Gestión de la Seguridad y Salud*. Oriente-Manabí Editorial. https://doi.org/10.63618/omeditorial/l30

Cada uno de los textos de OM Editorial han sido sometido a un proceso de evaluación por pares doble ciego externos (double-blind paper review) con base en la normativa del editorial.

Revisores:

Ing. Juan Manuel Guerrero Calero, PhD	Universidad Estatal del Sur de Manabí – Ecuador
Lic. Marvi Alexander Viteri Ruiz Mgs.	Pontificia Universidad Católica del Ecuador – Ecuador

Reseña de Autores

Chang-Gomez, Mario Andrew

Universidad Nacional de la Amazonía Peruana

mario.chang@unapiquitos.edu.pe

https://orcid.org/0009-0003-4287-5868

Ingeniero Químico egresado de la Universidad Nacional de la Amazonía Peruana (UNAP), con Maestría en Ciencias y Tecnologías Ambientales, mención en Industria del Petróleo y Medio Ambiente, y candidato a Doctor en Ciencias Ambientales. Es docente de la Facultad de Ingeniería Química de la UNAP. Su trabajo articula la analítica de datos, inteligencia artificial y Big Data con la identificación temprana de peligros, evaluación de riesgos y toma de decisiones en entornos industriales. Su producción académica integra ciencia, ingeniería, transformación digital y responsabilidad ambiental para promover entornos laborales seguros y sostenibles.

Malca-Salas, Gustavo Adolfo

Universidad Nacional de la Amazonía Peruana

gustavo.malca@unapiquitos.edu.pe

https://orcid.org/0000-0002-1272-7667

Ingeniero Químico con Maestría en Ciencias con mención en Ecología y Desarrollo. Doctor en Educación por la Universidad Alas Peruanas y candidato a Doctor en Ingeniería Química Ambiental por la Universidad Nacional de Trujillo. Es docente principal de la Facultad de Ingeniería Química de la Universidad Nacional de la Amazonía Peruana, donde imparte cursos relacionados con aspectos ambientales, Seguridad y Salud en el Trabajo y factores de riesgo en la industria. Es autor de investigaciones sobre energías alternativas, reducción de emisiones de CO_2, calidad del aire, huella de carbono y residuos sólidos.

Souza-Najar, Rosa Isabel

Universidad Nacional de la Amazonía Peruana

rosa.souza@unapiquitos.edu.pe

https://orcid.org/0000-0002-7359-3332

Ingeniera Química por la Universidad Nacional de la Amazonía Peruana (UNAP), con Maestría y Doctorado en Ingeniería Química Ambiental por la Universidad Nacional de Trujillo. Es docente de Química Analítica en la Facultad de Ingeniería Química de la UNAP. Posee experiencia en el estudio de compuestos bioactivos de plantas con potencial hipoglucemiante y en el asesoramiento de tesis sobre temas ambientales. Su trabajo integra la química aplicada, la analítica de datos y los enfoques sostenibles orientados a la prevención de riesgos y a los desafíos ambientales contemporáneos.

Araujo-Dávila, Carlos Enrique

Universidad Nacional de la Amazonía Peruana

caraujo@unapiquitos.edu.pe

https://orcid.org/0000-0003-0774-9287

Ingeniero Químico por la Universidad Nacional de la Amazonía Peruana, con grado de Magíster en Ciencias con mención en Ecología y Desarrollo Sostenible. Su perfil integra la ingeniería con enfoques ambientales orientados a la gestión sostenible de los recursos y la protección del entorno amazónico. Se desempeña como docente de Física y su trabajo académico se vincula con la seguridad industrial y el uso de inteligencia artificial para optimizar procesos, prevenir riesgos y mejorar la toma de decisiones. Promueve una ingeniería innovadora, segura y ambientalmente responsable..

Wong-Ramirez, Jandira del Pilar

Universidad Nacional de la Amazonía Peruana

jandira.wong@unapiquitos.edu.pe

https://orcid.org/0009-0001-3685-8231

Ingeniero Químico por la UNAP, titulado, colegiado y con Maestría. Cuenta con habilidades de liderazgo, trabajo en equipo y orientación a resultados. Posee 20 años de experiencia en minería subterránea y es especialista en gestión de aguas, incluyendo sistemas de tratamiento de agua de mina, aguas residuales domésticas y agua potable. Ha participado en auditorías de sistemas integrados de gestión ISO 45001 y 9001, fiscalizaciones de OEFA, OSINERGMIN y autoridades del agua, además de monitoreos participativos y manejo de documentación legal ambiental.

Vasquez-Pinedo, Jorge Armando

Universidad Nacional de la Amazonía Peruana

jorge.armando@unapiquitos.edu.pe

https://orcid.org/0000-0002-8811-4832

Ingeniero Químico por la Universidad Nacional de la Amazonía Peruana, Magíster en Gestión Pública y Doctor en Ciencias Empresariales por la misma institución. Su trayectoria académica y profesional integra la ingeniería, la investigación y la gestión estratégica, con énfasis en innovación, sostenibilidad y mejora continua. Ha desarrollado actividades de docencia, investigación y gestión, promoviendo la aplicación de soluciones tecnológicas orientadas al uso eficiente de los recursos y al desarrollo sostenible.

Casas-Tello, Dan Elias

Universidad Nacional de la Amazonía Peruana

dancasastello@gmail.com

https://orcid.org/0009-0006-3152-022X

Ingeniero Químico, MBA y docente de posgrado, con amplia experiencia en dirección de proyectos, ingeniería de procesos, operaciones industriales y gestión estratégica en el sector energético y de hidrocarburos. Ha liderado portafolios de inversión superiores a US$100 millones, integrando ingeniería, seguridad de procesos, evaluación financiera y sostenibilidad. Actualmente se desempeña como ejecutivo en Petroperú y docente de programas de maestría de la Universidad Nacional de la Amazonía Peruana. Sus líneas de investigación incluyen energía, hidrocarburos, evaluación de inversiones, contaminación ambiental y gestión de proyectos.

Ramírez-Álvarez, Karenth Elena

Universidad Nacional de la Amazonía Peruana

karenth.ramirez@unapiquitos.edu.pe

https://orcid.org/0000-0003-4786-7042

Ingeniero Químico, con Maestría en Ingeniería Ambiental y Desarrollo Sustentable por la Pontificia Universidad Católica Argentina y egresado del Doctorado en Ingeniería Industrial de la Universidad Nacional Mayor de San Marcos. Se desempeña como docente asociado de la Facultad de Ingeniería Química de la Universidad Nacional de la Amazonía Peruana, en el Departamento Académico de Ingeniería Química.

Vásquez-Gil, Oscar Alberto

Universidad Nacional de la Amazonía Peruana

oscar.vasquez@unapiquitos.edu.pe

https://orcid.org/0000-0001-7513-1441

Ingeniero Químico y Magíster con mención en Planificación y Manejo de Áreas Naturales Protegidas por la Universidad Nacional de la Amazonía Peruana. Es candidato a Doctor en Administración por la Universidad San Ignacio de Loyola. Cuenta con más de 20 años de experiencia en procesos industriales, hidrocarburos y sistemas integrados de gestión, además de una amplia trayectoria docente de pregrado y posgrado. Es especialista en procesamiento de bases de datos, diseño asistido por computadora, Power BI, soporte técnico y redes.

Carrasco-Montañez, Daniel Diomedes

Universidad Nacional de la Amazonía Peruana

dcarrasco@unapiquitos.edu.pe

https://orcid.org/0000-0002-2317-3911

Ingeniero Químico por la Universidad Nacional de la Amazonía Peruana, con estudios de Maestría en Ciencias en Ecología y Desarrollo Sostenible. Su trayectoria integra la ingeniería con enfoques ambientales orientados a la gestión sostenible de los recursos naturales. Está comprometido con la investigación y la aplicación de soluciones tecnológicas frente a los desafíos ecológicos, especialmente en contextos amazónicos. Su labor promueve prácticas que articulan el desarrollo productivo con la conservación del entorno, la innovación y la formación de profesionales conscientes del impacto ambiental de la ingeniería.

Índice

Índice de Figuras

Introducción

La prevención de riesgos laborales atraviesa una etapa de transformación que no se explica únicamente por la aparición de nuevas herramientas. Sensores, plataformas digitales, inteligencia artificial, Big Data, dispositivos portátiles y entornos de simulación están cambiando la forma de observar el trabajo, interpretar señales y organizar respuestas. Su aporte más valioso reside en ampliar la capacidad para reconocer condiciones peligrosas antes de que se conviertan en lesiones, enfermedades o pérdidas operacionales. Esta posibilidad modifica una práctica históricamente apoyada en registros posteriores al evento y abre espacio para una gestión más anticipatoria. Sin embargo, disponer de información en tiempo real o de modelos predictivos no garantiza por sí mismo una prevención más efectiva; el conocimiento técnico solo adquiere sentido cuando se traduce en decisiones oportunas, controles adecuados y mejoras verificables en las condiciones donde las personas desarrollan sus actividades.

El cambio digital ocurre, además, dentro de un mundo laboral que ya venía modificándose. La automatización, las plataformas, el teletrabajo, la reorganización de cadenas productivas y la convivencia entre personas y sistemas inteligentes han creado escenarios más variables, distribuidos e interdependientes. Algunos peligros tradicionales pueden disminuir cuando una máquina asume tareas repetitivas, pesadas o altamente expuestas, mientras surgen otros relacionados con la carga mental, la intensificación del ritmo, la vigilancia, la dependencia tecnológica o la pérdida de autonomía. La seguridad y salud en el trabajo necesita leer ambas caras del proceso sin idealizar la innovación ni rechazarla por principio. El desafío consiste en integrar sus capacidades dentro de una prevención que conserve la jerarquía de controles, reconozca los factores humanos y organizacionales y se mantenga atenta a los riesgos emergentes que acompañan cada cambio.

Transformar datos en inteligencia preventiva exige mucho más que almacenarlos. Una medición aislada de ruido, temperatura, movimiento, frecuencia cardiaca o proximidad ofrece una señal parcial; para comprenderla se necesita contexto, calidad, trazabilidad y una relación clara con la decisión que se pretende apoyar. La integración de fuentes ambientales, operacionales y

humanas permite reconocer patrones que antes permanecían dispersos, pero también introduce preguntas sobre representatividad, errores, interoperabilidad y uso legítimo. Los modelos de inteligencia artificial pueden clasificar imágenes, detectar desviaciones o estimar probabilidades, aunque sus resultados dependen de los datos, supuestos y condiciones bajo los cuales fueron desarrollados. Por ello, la analítica preventiva debe expresar incertidumbre, someterse a validación y conservar una supervisión profesional capaz de cuestionar la salida cuando el trabajo real no coincide con aquello que el sistema aprendió.

La implementación representa el punto en el que una promesa tecnológica se encuentra con la realidad cotidiana. Una solución técnicamente precisa puede fracasar si interfiere con equipos de protección, genera demasiadas alertas, exige conectividad inexistente o llega a un equipo que no tiene autoridad para actuar. Escuchar antes de diseñar permite reconocer necesidades, expectativas y temores, así como comprender procedimientos informales que sostienen la operación. La participación de los trabajadores no debería limitarse a una prueba final de usabilidad, porque quienes viven el riesgo conocen variaciones, restricciones y señales que rara vez aparecen en una especificación comercial. Incorporar esa experiencia desde la definición del problema favorece soluciones más comprensibles, accesibles e inclusivas, adaptadas a la diversidad de cuerpos, capacidades, idiomas, contratos, turnos y territorios que integran el trabajo contemporáneo.

La ruta que conduce desde una alerta hasta una acción requiere responsabilidades definidas. Detectar un peligro no equivale a controlarlo: alguien debe recibir la información, comprender su gravedad, disponer de autoridad, coordinar recursos y verificar el cierre. Cuando esta cadena permanece implícita, la digitalización produce notificaciones sin respuesta o transfiere al trabajador la carga de compensar fallas del sistema. Las tecnologías preventivas deben integrarse con mantenimiento, operación, salud ocupacional, emergencias y dirección, de manera que cada nivel de criticidad tenga una conducta asociada. Los simulacros, la revisión de incidentes y el seguimiento de tiempos ayudan a comprobar el recorrido completo. El desempeño de una plataforma no se mide entonces por el número de avisos emitidos, sino por su

capacidad para activar controles eficaces, reducir exposiciones y sostener el aprendizaje organizacional.

La innovación también plantea decisiones éticas que afectan confianza y legitimidad. Los sistemas pueden reproducir sesgos presentes en datos históricos, ofrecer explicaciones insuficientes o funcionar de manera desigual entre grupos. El monitoreo continuo amplía la capacidad preventiva y, al mismo tiempo, puede invadir privacidad si la finalidad no está delimitada. La conectividad facilita coordinación, pero incorpora vulnerabilidades capaces de alterar señales o dejar indisponibles funciones críticas. Gobernar estas tensiones exige reglas sobre datos, modelos, accesos, actualizaciones, proveedores, incidentes y mecanismos de impugnación. La responsabilidad no desaparece cuando una decisión se automatiza; se distribuye entre quienes diseñan, compran, configuran, supervisan y utilizan la tecnología. Esa distribución debe estar documentada sin volverse difusa, especialmente cuando una salida puede influir sobre la salud, la asignación de tareas o los derechos de una persona.

Este libro recorre la transformación digital de la prevención desde sus fundamentos hasta los escenarios que empiezan a configurarse. El primer capítulo sitúa los cambios del trabajo y la necesidad de una prevención capaz de anticiparse; el segundo examina datos, sensores, Big Data, inteligencia artificial, visualización y simulación; el tercero traslada la innovación al lugar donde ocurre la actividad, con énfasis en madurez organizacional, participación y coordinación; el cuarto aborda ética, privacidad, ciberseguridad, gobernanza y capacidades futuras. La secuencia no propone una adopción tecnológica uniforme, sino un criterio para decidir cuándo, cómo y para quién una solución aporta valor. La transformación será preventiva en la medida en que fortalezca el control sobre los peligros, haga más comprensible la incertidumbre y permita cuidar mejor a las personas sin reducirlas a registros, puntajes o patrones de comportamiento.

Capítulo I: Prevenir en un mundo laboral que está cambiando

Prevenir en un mundo laboral que está cambiando

La prevención de riesgos laborales nació, en buena medida, de la necesidad de comprender hechos ya consumados: una lesión, una enfermedad, una avería o una pérdida operacional. Investigar esos acontecimientos sigue siendo indispensable, pero el trabajo contemporáneo obliga a ampliar la mirada. Las organizaciones operan hoy mediante redes de personas, equipos automatizados, plataformas digitales, proveedores y decisiones distribuidas que cambian con rapidez. En ese entorno, esperar a que el daño haga visible una debilidad supone llegar tarde. El reto consiste en reconocer cómo se está configurando el riesgo mientras el trabajo ocurre y actuar antes de que una combinación adversa produzca consecuencias.

La magnitud del problema ayuda a situar esta transición. Las estimaciones más recientes de la Organización Internacional del Trabajo, referidas a 2019, atribuyen aproximadamente 2,93 millones de muertes anuales a factores relacionados con el trabajo y calculan que 395 millones de personas sufren lesiones laborales no mortales cada año. La mayor parte de la mortalidad corresponde a enfermedades relacionadas con el trabajo, no a accidentes repentinos, lo cual revela los límites de una gestión concentrada en eventos visibles y de aparición inmediata (Organización Internacional del Trabajo [OIT], 2023). Prevenir exige observar exposiciones acumulativas, condiciones organizacionales, cambios tecnológicos y señales débiles que rara vez aparecen completas en un único registro.

La transformación digital ofrece nuevas capacidades para esa tarea. Sensores conectados, dispositivos portátiles, visión computacional, procesamiento de lenguaje natural y modelos predictivos pueden integrar información antes dispersa, detectar desviaciones y apoyar decisiones oportunas. Sin embargo, digitalizar no equivale automáticamente a prevenir. Un sistema puede recopilar millones de datos y seguir sin comprender el contexto de una tarea; también puede introducir vigilancia, presión, sesgos o una falsa sensación de control. La OIT (2025) reconoce ambas dimensiones: la inteligencia artificial, la robótica y los sistemas inteligentes pueden apartar a las personas de operaciones

peligrosas y mejorar el monitoreo, pero su implantación también genera riesgos ergonómicos, psicosociales, de privacidad y de responsabilidad.

Este capítulo propone una idea central: la prevención inteligente no se define por la cantidad de tecnología incorporada, sino por la capacidad de combinar datos, conocimiento del trabajo y juicio profesional para intervenir de manera anticipada. Esa capacidad depende tanto de la infraestructura digital como de la confianza, el liderazgo y la participación de quienes realizan las tareas. Los datos amplían el campo de observación; la experiencia humana permite interpretarlos, cuestionarlos y convertirlos en acciones con sentido.

La distinción entre digitalización y transformación ayuda a comprender el alcance. Digitalizar puede significar sustituir una hoja en papel por un formulario electrónico. La transformación aparece cuando esa información se conecta con decisiones, altera responsabilidades, reduce tiempos de respuesta y permite aprender entre áreas. El cambio no es neutral: modifica qué se vuelve visible, quién puede decidir y cómo se evalúa el desempeño. Por eso debe gestionarse como una intervención organizacional y no solo como un proyecto informático.

También es necesario evitar dos extremos. El primero idealiza los datos y supone que una organización podrá eliminar la incertidumbre si mide lo suficiente. El segundo rechaza la analítica porque el trabajo siempre contiene variabilidad. Una prevención madura reconoce que ningún modelo captura la totalidad del sistema, pero aprovecha la información disponible para formular mejores hipótesis y asignar recursos. La incertidumbre no invalida la decisión; exige hacer explícitos sus límites, documentar los supuestos y revisar los resultados con evidencia obtenida durante la operación.

Esta postura sitúa a la tecnología dentro de la ética del cuidado. El objetivo no es vigilar a las personas para exigirles una conducta perfecta, sino diseñar condiciones que toleren errores razonables, detecten degradaciones y reduzcan exposición. La pregunta decisiva no es cuánto puede observar una organización, sino cuánto necesita observar para proteger, con qué garantías y para beneficio de quién.

1.1. Cuando la prevención deja de ser solamente reactiva

Una gestión reactiva aprende después del acontecimiento. Examina causas, determina incumplimientos, calcula tasas y establece acciones correctivas. Esta lógica ha contribuido a mejorar procesos y conserva una función legítima: los accidentes y las enfermedades contienen información que no debe desaprovecharse. El problema aparece cuando el desempeño preventivo se reduce a indicadores retrospectivos, como el número de lesiones, los días perdidos o los costos de siniestralidad. Tales métricas describen resultados finales, pero dicen poco sobre la calidad actual de los controles, la capacidad de respuesta o las condiciones que están acumulando vulnerabilidad.

Las tasas bajas, además, admiten interpretaciones distintas. Pueden reflejar controles eficaces, una etapa sin eventos pese a exposiciones persistentes, subregistro o simple variación aleatoria. Cuando el número de accidentes es pequeño, su ausencia tampoco ofrece suficiente sensibilidad para orientar decisiones cotidianas. La revisión de Ali et al. (2022) sobre indicadores de seguridad en industrias de servicios públicos distingue indicadores retrospectivos y diferentes clases de indicadores adelantados; sus hallazgos muestran que una evaluación más completa requiere combinar medidas objetivas y subjetivas, integrar la gestión del riesgo y comprobar la relación real entre las métricas seleccionadas y los resultados de seguridad.

Abandonar una prevención exclusivamente reactiva no implica desechar la estadística de accidentes. Significa ubicarla dentro de un sistema de información más amplio. Una organización necesita saber qué ocurrió, pero también si las barreras críticas están disponibles, si las inspecciones detectan desviaciones relevantes, si los cambios se evalúan antes de implementarse, si las personas pueden reportar problemas y si las respuestas llegan a tiempo. La conversación cambia de “¿cuántos accidentes tuvimos?” a “¿qué condiciones están aumentando o reduciendo nuestra capacidad de trabajar con seguridad?”.

Esta evolución modifica el papel del profesional preventivo. Ya no actúa únicamente como investigador posterior o custodio del cumplimiento, sino como integrador de señales procedentes de operaciones, mantenimiento, salud ocupacional, recursos humanos y tecnología. Su función incluye formular buenas

preguntas, evaluar la calidad de los datos y reconocer que un indicador puede mejorar por razones ajenas a una reducción real del riesgo. También debe preservar una frontera ética: la información reunida para proteger la salud no debería transformarse, sin reglas transparentes, en un mecanismo de sanción o evaluación individual.

1.1.1. De registrar accidentes a anticipar escenarios

Anticipar no significa adivinar el futuro ni asignar a cada trabajador una probabilidad de accidentarse. Consiste en construir escenarios plausibles a partir de exposiciones, cambios, interacciones y desempeño de controles. Un escenario preventivo relaciona, por ejemplo, el aumento de temperatura ambiental, la duración de la jornada, la carga física, el uso de equipos de protección y la disponibilidad de pausas. Ninguna variable explica por sí sola un desenlace; su combinación permite identificar cuándo el margen de seguridad se está reduciendo.

El Big Data amplía las posibilidades de análisis porque incorpora volumen, velocidad y variedad de información. Registros de mantenimiento, alarmas, permisos de trabajo, condiciones ambientales, turnos, observaciones y reportes narrativos pueden analizarse en conjunto. La utilidad no proviene de acumularlos, sino de organizar preguntas preventivas y convertir hallazgos en decisiones. Un modelo que alerta sobre una posible falla, pero no activa una revisión, no modifica la exposición. Del mismo modo, una predicción precisa sobre fatiga pierde valor si la organización mantiene cargas y horarios incompatibles con la recuperación.

La IA puede contribuir en varios niveles. La visión computacional identifica proximidad entre personas y maquinaria o posturas potencialmente exigentes; los modelos de series temporales reconocen cambios en vibración, temperatura o gases; el procesamiento de lenguaje natural agrupa temas en reportes de incidentes y observaciones; los algoritmos de clasificación ayudan a priorizar inspecciones. El-Helaly (2024) describe aplicaciones basadas en sensores y dispositivos portátiles para el monitoreo continuo, junto con limitaciones asociadas con privacidad, seguridad de los datos, precisión y efectos sobre la

autonomía. La evidencia disponible aconseja tratar estas herramientas como apoyo y no como autoridad incuestionable.

Una revisión sistemática reciente encontró un desarrollo creciente de aplicaciones de IA en seguridad y salud, especialmente en sectores industriales, aunque también señala heterogeneidad metodológica, problemas de estandarización y desafíos éticos y operativos (La Torre et al., 2026). Esa distancia entre capacidad técnica y evidencia de impacto es importante. Detectar una postura, clasificar una imagen o predecir una categoría de riesgo no equivale por sí mismo a demostrar una reducción sostenida de lesiones o enfermedades. Los modelos deben evaluarse por su desempeño técnico y por su contribución a resultados preventivos, considerando falsos positivos, omisiones, transferibilidad y consecuencias no previstas.

La anticipación funciona mejor cuando se organiza en ciclos breves: observar, interpretar, decidir, intervenir y aprender. Durante la observación se integran datos técnicos y relatos del trabajo; la interpretación determina si la señal representa una variación esperable o una degradación; la decisión asigna prioridad y responsable; la intervención modifica el proceso, y el aprendizaje comprueba si el control produjo el efecto deseado. La automatización puede acelerar las primeras etapas, pero la responsabilidad debe permanecer claramente definida.

La selección de variables merece especial cuidado. Utilizar edad, sexo, condición de salud o historial individual para predecir conductas puede generar discriminación y desviar la atención desde las condiciones controlables hacia características personales. En prevención resulta preferible modelar exposiciones, tareas, desempeño de barreras y condiciones operacionales, aplicando minimización de datos y revisiones de equidad. Cuando una variable sensible sea indispensable para comprobar que un control protege de manera equivalente a distintos grupos, su uso debe quedar justificado, limitado y protegido.

Los modelos necesitan una línea de base comprensible. Antes de desplegar aprendizaje automático conviene comprobar qué decisiones pueden lograrse mediante reglas, tendencias o análisis descriptivo. Esta comparación evita

atribuir a la IA mejoras que provienen de ordenar la información o responder con mayor disciplina. Un sistema complejo se justifica cuando aporta capacidad demostrable frente a una alternativa más sencilla, sin imponer costos de mantenimiento, dependencia o explicación desproporcionados.

1.1.2. Aprender de las señales antes de que ocurra el daño

Los cuasiaccidentes, las desviaciones y las dificultades para completar una tarea constituyen señales valiosas porque revelan cómo una situación pudo haber terminado de otra manera. Haas et al. (2020), al analizar reportes de cuasiaccidentes elaborados por trabajadores de la minería, muestran que estos registros pueden aportar información sobre causas potenciales y promover iniciativas de gestión. Su valor depende de que el reporte sea comprendido como una oportunidad de aprendizaje y no como una confesión de culpa.

Una señal débil suele ser ambigua: una alarma intermitente, una protección que incomoda, una maniobra que exige improvisar o una secuencia que solo funciona cuando el equipo está completo. Considerada aisladamente, puede parecer menor. Repetida en distintos turnos o relacionada con mantenimiento diferido, presión de producción y fatiga, adquiere otro significado. La analítica ayuda a reunir esos fragmentos, pero el sistema debe conservar suficiente detalle para no eliminar el contexto en nombre de la estandarización.

El número de reportes tampoco puede interpretarse de forma lineal. Un aumento puede expresar deterioro operacional o una mejora de la confianza para informar. Penalizar áreas por reportar más produce el incentivo equivocado: reduce la visibilidad sin eliminar la exposición. Conviene observar, junto al volumen, la calidad de los reportes, la diversidad de riesgos identificados, el tiempo de respuesta, la proporción de acciones cerradas con verificación y la retroalimentación recibida por quienes alertaron.

Las señales no proceden únicamente de incidentes. El uso frecuente de atajos, las horas extraordinarias, la rotación, las quejas musculoesqueléticas, las fallas repetitivas, la presión de tiempos y las dudas expresadas durante una charla pueden anticipar problemas. La OMS (2022) subraya que las intervenciones sobre salud mental deben actuar sobre las condiciones organizacionales —carga, horario, control, violencia y apoyo— y contar con la participación

significativa de trabajadores y representantes. Esta orientación evita reducir el riesgo psicosocial a la capacidad individual para soportar entornos mal diseñados.

Aprender temprano demanda una disciplina de seguimiento. Cada señal necesita una clasificación proporcionada, una persona responsable y un criterio de cierre; las alertas críticas exigen respuesta inmediata, mientras otras se agregan para observar patrones. El cierre administrativo no basta: debe verificarse que la acción disminuyó el riesgo y no lo desplazó. Un tablero digital puede facilitar esta trazabilidad, siempre que no convierta el proceso en una carrera por marcar tareas como completadas.

La respuesta a una señal debería conservar su vínculo con la jerarquía de controles. Ante una exposición recurrente, entregar otra capacitación o emitir un recordatorio puede ser rápido, aunque insuficiente si el peligro puede eliminarse, sustituirse o aislarse mediante ingeniería. La analítica aporta valor cuando ayuda a dirigir recursos hacia controles de mayor eficacia y permite comprobar su desempeño; usada solo para reforzar vigilancia conductual, corre el riesgo de modernizar una respuesta débil.

También conviene diferenciar señal y umbral. No todas las variaciones requieren detener una operación, pero algunas combinaciones justifican una intervención automática. Los criterios deben establecerse antes de observar el resultado y revisarse con datos de desempeño. Umbrales demasiado sensibles producen fatiga de alarmas; umbrales laxos normalizan la desviación. La calibración necesita especialistas del proceso y personas expuestas, pues ambos conocen consecuencias que una base histórica puede no contener.

1.2. Transformación digital y nuevas formas de cuidar

La transformación digital no es la incorporación aislada de software. Supone modificar la forma en que una organización produce información, coordina decisiones y aprende. En prevención, ese cambio puede conectar datos ambientales, operativos y humanos para construir una visión más oportuna del trabajo. También puede fragmentar responsabilidades cuando la tecnología se implementa sin gobernanza, se contrata como una solución cerrada o se separa de los sistemas existentes de seguridad y salud.

Los sistemas digitales inteligentes abarcan sensores de gases, ruido, temperatura y movimiento; dispositivos portátiles; cámaras; robots; drones; aplicaciones móviles; gemelos digitales y entornos de realidad virtual. EU-OSHA (2025a) los define como sistemas que recopilan y analizan datos para identificar peligros, evaluar riesgos y prevenir o minimizar daños. La misma agencia enfatiza principios de diseño relacionados con seguridad de la información, privacidad, confiabilidad, inclusión, integración con la gestión preventiva y participación de los usuarios.

Su aporte más evidente es ampliar la observación. Una medición periódica ofrece una fotografía; un sensor continuo permite reconocer tendencias y exposiciones transitorias. Un recorrido presencial examina una zona en un momento concreto; un dron puede inspeccionar lugares de difícil acceso sin exponer directamente a una persona. La realidad virtual permite ensayar respuestas ante emergencias poco frecuentes, y un modelo de mantenimiento predictivo puede alertar sobre degradaciones antes de una falla. Estas aplicaciones resultan valiosas cuando respetan la jerarquía de controles: la tecnología debería favorecer la eliminación, sustitución o control del peligro, no limitarse a avisar al individuo que debe protegerse.

La digitalización también cambia la naturaleza del cuidado. En un enfoque tradicional, la protección suele expresarse como norma, equipo o supervisión. En un entorno conectado, cuidar implica gobernar datos: decidir qué se recopila, con qué finalidad, durante cuánto tiempo, quién accede, cómo se corrigen errores y qué usos quedan prohibidos. Los datos de salud, ubicación o comportamiento pueden ser particularmente sensibles. EU-OSHA (2025a) recomienda evitar que la información reunida por sistemas preventivos se utilice para evaluar el desempeño individual, porque esa transferencia de propósito puede deteriorar la confianza y trasladar la responsabilidad hacia el trabajador.

El riesgo de una finalidad expansiva es real. Un dispositivo instalado para detectar caídas puede terminar midiendo pausas; una cámara destinada a identificar ingreso a zonas peligrosas puede utilizarse para puntuar productividad; un algoritmo de turnos puede optimizar cobertura y, al mismo tiempo, reducir recuperación. La gestión algorítmica automatiza o apoya

funciones antes realizadas por supervisores, como asignar tareas, vigilar y evaluar. La OCDE (2025a) reconoce posibles ganancias de eficiencia y consistencia, junto con impactos adversos que dependen del diseño y del contexto de uso.

Las tecnologías deben evaluarse antes de la compra y durante todo su ciclo de vida. La evaluación inicial incluye propósito preventivo, población afectada, escenario de falla, validez de los datos y compatibilidad con otros controles. La fase piloto necesita participación de usuarios reales, pruebas en condiciones diversas y criterios de suspensión. Durante la operación deben medirse precisión, tasa de falsas alarmas, cambios en la carga de trabajo, aceptación y resultados preventivos. Al retirarse el sistema, la organización debe definir el destino de los datos y conservar la capacidad de explicar decisiones pasadas.

Un marco útil para la gobernanza es el AI Risk Management Framework del National Institute of Standards and Technology, que organiza la gestión en cuatro funciones: gobernar, mapear, medir y gestionar. También identifica características de confianza como validez, confiabilidad, seguridad, resiliencia, transparencia, explicabilidad, privacidad y equidad (Tabassi, 2023). Aunque no fue creado específicamente para la prevención laboral, ayuda a traducir principios éticos en responsabilidades y pruebas concretas.

La regulación internacional confirma que la IA en el trabajo no es una cuestión meramente técnica. El Reglamento de Inteligencia Artificial de la Unión Europea clasifica como de alto riesgo diversos sistemas utilizados en empleo y gestión de trabajadores, y prohíbe ciertos usos de inferencia emocional en el lugar de trabajo, salvo excepciones médicas o de seguridad (Unión Europea, 2024). Su aplicación directa varía según la jurisdicción, pero la orientación es relevante para América Latina: cuando una herramienta afecta derechos, salud o decisiones laborales, requiere trazabilidad, supervisión humana y mecanismos de impugnación.

La región afronta, además, desigualdades de infraestructura, madurez digital, formalización y capacidad institucional. Una solución diseñada con datos abundantes y conectividad estable puede fallar en una pequeña empresa, una operación rural o una cadena con alta informalidad. La pertinencia tecnológica

debe evaluarse respecto de recursos, competencias, mantenimiento y condiciones locales. A veces, una aplicación sencilla para reportar peligros y recibir respuesta genera más valor que un modelo sofisticado sin datos confiables.

El catálogo de Oriente-Manabí Editorial contiene una obra relacionada, *Salud integral en la era digital: Bienestar físico, mental y ocupacional desde un enfoque preventivo*, que reúne aproximaciones a salud digital, bienestar y prevención y documenta literatura sobre plataformas e indicadores de seguridad y salud (González-Naranjo et al., 2026). Su pertinencia para este capítulo radica en el enfoque preventivo e interdisciplinario; se incorpora como contexto editorial regional, sin atribuirle evidencia que corresponde a los estudios originales que compila.

La madurez digital preventiva puede entenderse como una progresión, no como una competencia por acumular herramientas. En un nivel inicial, la prioridad es disponer de definiciones consistentes, reportes accesibles y responsabilidades de respuesta. Después pueden integrarse bases, automatizar alertas y desarrollar visualizaciones. Los modelos predictivos requieren etapas adicionales de calidad, validación, gobernanza y competencias. Saltar directamente a la predicción suele trasladar al algoritmo las inconsistencias que ya existían en los registros.

Esta progresión protege a pequeñas y medianas empresas de soluciones sobredimensionadas. Una organización puede iniciar con un inventario de fuentes, un diccionario de datos, indicadores vinculados con controles críticos y reuniones periódicas de aprendizaje. Si esas prácticas funcionan, la automatización puede aliviar tareas y ampliar cobertura. Sin una rutina para decidir y actuar, el tablero más avanzado se convierte en una pantalla adicional.

La interoperabilidad plantea otro desafío. Los datos preventivos proceden de sistemas con propietarios, frecuencias y formatos distintos. Integrarlos exige identificadores, reglas de calidad y control de versiones, pero también acuerdos sobre finalidad y acceso. No todo dato técnicamente disponible debe combinarse. La posibilidad de enlazar salud, ubicación, productividad y

desempeño aumenta la capacidad analítica y, simultáneamente, el riesgo de inferencias invasivas.

1.3. Comprender el riesgo más allá de las estadísticas

Los indicadores condensan la realidad para hacerla manejable. Esa reducción es necesaria, pero puede ocultar diferencias entre tareas, colectivos y momentos. Dos centros con una tasa similar de lesiones pueden tener exposiciones y capacidades preventivas muy distintas. Incluso dentro de una planta, el promedio de ruido, temperatura o carga puede esconder picos breves que afectan a un grupo específico. Comprender el riesgo exige preguntar qué representa el dato, cómo fue producido y qué quedó fuera.

El dato no es la realidad misma; es un registro generado mediante una definición, un instrumento y una decisión. Una lesión puede no aparecer porque no se informó, una exposición puede quedar fuera por falta de medición y un reporte narrativo puede perder información al convertirse en una categoría cerrada. Por eso, la calidad incluye exactitud y completitud, pero también representatividad, oportunidad, trazabilidad y adecuación al uso.

La analítica permite cruzar fuentes y descubrir relaciones que no son evidentes. Sin embargo, una correlación no demuestra causalidad. Si los accidentes aumentan durante horas extraordinarias, es necesario examinar fatiga, complejidad, supervisión, dotación y tipo de tarea. Un algoritmo puede encontrar asociaciones históricas que reflejan decisiones organizacionales o desigualdades previas. Utilizarlas sin interpretación puede reproducir el problema bajo una apariencia objetiva.

La incertidumbre debería aparecer en los resultados. Una probabilidad presentada como número exacto puede sugerir una precisión que el modelo no posee, sobre todo cuando existen pocos eventos, cambios en el proceso o datos incompletos. Rangos, niveles de confianza y advertencias sobre aplicabilidad ayudan a evitar decisiones automáticas. Para usuarios operacionales suele ser más útil conocer qué factores impulsan una alerta y qué acción se recomienda que recibir una puntuación aislada.

Comparar unidades requiere precaución. Una tasa ajustada por horas trabajadas mejora la comparación, pero no controla diferencias en peligros, exposición, subcontratación o registro. Los rankings pueden incentivar ocultamiento y competencia improductiva. Una alternativa consiste en utilizar referentes para abrir una investigación conjunta: qué prácticas explican la diferencia, qué datos faltan y qué controles pueden transferirse sin ignorar el contexto.

1.3.1. Riesgos visibles y amenazas silenciosas

Los riesgos visibles una pieza sin resguardo, un derrame o un trabajo en altura suelen movilizar respuesta porque su relación con el daño es imaginable. Las amenazas silenciosas se acumulan: exposición química de baja intensidad, ruido, movimientos repetitivos, jornadas extensas, falta de control, hostigamiento o recuperación insuficiente. Las cifras de la OIT muestran que las enfermedades generan una proporción mucho mayor de muertes relacionadas con el trabajo que los accidentes fatales (OIT, 2023). Esta distribución obliga a equilibrar la atención entre seguridad inmediata y salud a largo plazo.

La digitalización añade riesgos poco visibles. La hiperconectividad puede extender la jornada; la automatización puede empobrecer tareas o generar carga cognitiva; una interfaz mal diseñada puede aumentar errores; el monitoreo continuo puede producir presión y pérdida de autonomía. La OMS (2024) identifica entre los riesgos psicosociales las cargas excesivas, los horarios prolongados o inflexibles, la falta de control, la supervisión autoritaria, la violencia, la inseguridad laboral y la escasa claridad de rol. Varias de estas condiciones pueden intensificarse mediante sistemas digitales aunque no dejen una huella inmediata en las tasas de accidentes.

La gestión algorítmica merece atención porque combina observación y decisión. Vignola et al. (2023) explican que puede afectar dimensiones de la calidad del empleo vinculadas con la salud: carga de trabajo, estabilidad de horarios e ingresos, autonomía, relaciones y confianza. Un sistema que aumenta el ritmo para optimizar productividad puede elevar la exposición musculoesquelética o reducir pausas; si sus criterios son opacos, la persona tampoco dispone de una vía clara para explicar circunstancias excepcionales.

Reconocer amenazas silenciosas requiere fuentes diferentes. La vigilancia ambiental y de salud aporta mediciones; las encuestas detectan percepciones; las entrevistas y grupos de discusión revelan mecanismos; los datos de ausentismo y rotación sugieren tendencias, aunque no explican por sí solos sus causas. La triangulación evita convertir un único indicador en diagnóstico. También protege frente al error de asumir que lo medible es necesariamente lo más importante.

1.3.2. El contexto detrás de cada dato

Un reporte adquiere significado cuando se reconstruye la situación en que fue producido. La frase “no usó el procedimiento” es insuficiente sin saber si el documento estaba actualizado, si podía ejecutarse con los recursos disponibles, si entraba en conflicto con metas de producción o si el equipo había aprendido una adaptación que permitía resolver una variabilidad no prevista. El objetivo no es justificar cualquier desviación, sino comprender por qué una conducta tuvo sentido para quien actuó.

Los datos históricos suelen heredar la lógica del sistema que los generó. Si durante años se registraron causas como “acto inseguro”, un modelo entrenado con esas etiquetas aprenderá a reproducir una atribución centrada en el individuo. Si ciertos contratistas reportan menos porque temen consecuencias, aparecerán artificialmente como más seguros. La preparación de datos debe revisar definiciones, valores faltantes, cambios de criterio y sesgos de selección antes de construir predicciones.

El contexto temporal también importa. Una alerta durante una puesta en marcha, una emergencia o un cambio de turno no tiene el mismo significado que durante operación estable. Conviene incorporar información sobre fase del proceso, dotación, mantenimiento, clima, carga, modificaciones recientes y experiencia del equipo. Esta contextualización mejora el análisis y reduce el riesgo de respuestas genéricas.

En materia preventiva, la explicabilidad no exige que todas las personas comprendan las matemáticas del modelo, pero sí que sepan qué información utiliza, qué significa la salida, cuáles son sus límites y cómo cuestionarla. Una supervisora necesita conocer por qué se priorizó una inspección; un trabajador

debe poder corregir un dato erróneo; el comité de seguridad debe acceder a información suficiente para evaluar efectos colectivos. La opacidad debilita tanto la legitimidad como el aprendizaje.

1.3.3. Factores humanos, organizacionales y tecnológicos

La expresión “factor humano” se ha usado con frecuencia como sinónimo de error individual. Esa reducción pierde de vista que la conducta surge de una interacción entre capacidades, diseño, información, presión, herramientas y organización. La persona se adapta a variaciones para que el sistema funcione; esas adaptaciones pueden sostener la producción y, bajo otra combinación de condiciones, contribuir a un incidente. Analizarlas permite intervenir sobre el sistema en lugar de limitarse a pedir mayor atención.

Los factores humanos incluyen carga física y mental, percepción, fatiga, experiencia, formación y comunicación. Los organizacionales abarcan prioridades, recursos, incentivos, contratación, liderazgo, aprendizaje y gestión del cambio. Los tecnológicos comprenden confiabilidad, interfaz, automatización, mantenimiento, ciberseguridad e interoperabilidad. Ninguno opera de forma aislada. Una alarma técnicamente precisa puede fracasar si se presenta en un momento de saturación, si produce alertas repetitivas o si la respuesta esperada entra en conflicto con otra instrucción.

El enfoque sociotécnico resulta particularmente útil ante la IA. No basta con validar el modelo; debe evaluarse el conjunto formado por datos, usuarios, proceso y gobernanza. Las preguntas relevantes incluyen quién decide después de la alerta, qué ocurre cuando la herramienta se equivoca, cómo se documenta una excepción y si la automatización modifica la distribución de responsabilidad. EU-OSHA (2024a) advierte que la gestión de trabajadores mediante IA puede mejorar ciertos procesos y, a la vez, producir consecuencias negativas para la seguridad y la salud.

La automatización también crea nuevas competencias. El personal necesita interpretar alertas y reconocer fallas del sistema, mientras especialistas en datos deben comprender el proceso laboral y sus consecuencias. La formación no puede reducirse al uso de la interfaz; debe incluir límites, privacidad, sesgos, ciberseguridad y procedimientos de contingencia. Cuando la tecnología deja de

estar disponible, la operación necesita conservar capacidades para trabajar de forma segura.

La ciberseguridad forma parte de la seguridad operacional. Un sensor manipulado, una interrupción de comunicaciones o una actualización defectuosa puede alterar una decisión preventiva. Los sistemas deben disponer de control de accesos, registro de cambios, respaldo, pruebas y mecanismos de funcionamiento seguro ante fallas. El principio de mínima recopilación ayuda en ambos frentes: recoger solo los datos necesarios reduce exposición y facilita gobernanza.

Un aspecto menos visible es la reorganización del trabajo provocada por la propia herramienta. Si un sistema genera cientos de alertas, alguien debe revisarlas; si introduce una nueva pantalla, compite por atención con otras fuentes; si requiere cargar datos manualmente, aumenta la carga administrativa. La evaluación debe incluir a quienes operan, supervisan, mantienen y auditan, porque los efectos pueden desplazarse entre funciones. Una mejora local no es preventiva cuando transfiere riesgo o sobrecarga a otra parte del sistema.

Los cambios tecnológicos necesitan tratarse mediante gestión del cambio. Antes del despliegue se deben identificar nuevas tareas, fallas posibles, competencias, dependencias y situaciones de emergencia. Después conviene observar el trabajo real y actualizar la evaluación. La versión del algoritmo o del software es parte de esa gestión: una actualización puede alterar sensibilidad, interfaz o comportamiento sin modificar físicamente el equipo.

1.4. La experiencia del trabajador como fuente de conocimiento

Quien realiza una tarea conoce variaciones que rara vez aparecen en el procedimiento: una herramienta que se atasca, una instrucción ambigua, un pico de demanda, una coordinación difícil o un control que funciona solo en condiciones ideales. Este conocimiento práctico no reemplaza mediciones ni normas, pero permite interpretar por qué el trabajo real se aparta del trabajo prescrito. Integrarlo mejora la identificación de peligros y la calidad de las soluciones.

La participación suele confundirse con informar al personal después de haber decidido. Una participación sustantiva empieza antes: trabajadores y representantes contribuyen a definir el problema, seleccionar datos, probar herramientas, evaluar impactos y revisar resultados. ISO 45001 sitúa la consulta y participación junto con el liderazgo como componentes del sistema de gestión (International Organization for Standardization [ISO], 2018). La OMS (2022) formula una orientación semejante para la salud mental en el trabajo al recomendar la intervención significativa de trabajadores y personas con experiencia vivida.

La información cualitativa puede analizarse de manera sistemática. Los relatos de cuasi accidentes, comentarios de inspecciones y reuniones de inicio contienen vocabulario, secuencias y condiciones. El procesamiento de lenguaje natural ayuda a clasificar temas, detectar recurrencias y priorizar revisión, pero no debería borrar la voz original. Los resultados automatizados requieren muestreo manual, validación con usuarios y posibilidad de reclasificación.

La experiencia también ayuda a descubrir variables ausentes. Un modelo puede asociar un turno con mayor riesgo y omitir que allí se concentran tareas de arranque, personal nuevo o equipos con mantenimiento pendiente. Conversar con el equipo convierte una asociación en una hipótesis operativa y evita intervenir sobre el atributo equivocado. El dato orienta la pregunta; el conocimiento situado contribuye a responderla.

Para que las personas compartan información necesitan percibir utilidad y protección. Si los reportes desaparecen en un sistema sin respuesta o se usan para sancionar, la participación se retrae. La retroalimentación debe indicar qué se entendió, qué se hará, por qué algunas propuestas no se adoptan y cómo se comprobará el resultado. Esta devolución transforma el reporte en un ciclo de aprendizaje.

La participación no elimina el conflicto. Operaciones, prevención, tecnología y trabajadores pueden valorar de manera diferente una solución. Un proceso maduro hace visibles esas diferencias y establece criterios: reducción de exposición, factibilidad, privacidad, carga adicional y equidad. La decisión final

debe quedar documentada y ser revisable, sobre todo cuando un sistema automatizado afecta ritmos, pausas o evaluación.

La inclusión merece un tratamiento específico. Los sistemas deben funcionar para diversidad de cuerpos, edades, idiomas, niveles de alfabetización, condiciones de salud y formas de contratación. Un dispositivo portátil que no se ajusta correctamente, una alarma basada solo en color o una aplicación inaccesible puede excluir a parte de la fuerza laboral. Probar con usuarios diversos no es una cortesía de diseño; es un requisito de eficacia preventiva.

La participación debe reconocer asimetrías de poder. Una persona puede aceptar un dispositivo porque teme perder una oportunidad laboral, no porque considere legítima la recopilación. Por ello, el consentimiento individual rara vez basta como fundamento único en la relación de trabajo. Se necesitan acuerdos colectivos, consulta con representantes, finalidades delimitadas y garantías que no dependan de la voluntad del supervisor inmediato. Los canales anónimos pueden complementar la conversación, aunque no sustituyen una cultura en la que sea seguro hablar abiertamente.

El conocimiento de trabajadores contratistas, temporales y de plataformas merece igual atención. Estos grupos suelen enfrentar exposiciones altas y menor capacidad para influir en el diseño del trabajo; también pueden quedar fragmentados entre sistemas de información de varias empresas. La organización que controla el proceso debe establecer mecanismos para recibir sus señales, coordinar respuestas y evitar que los límites contractuales se conviertan en vacíos preventivos.

Convertir la experiencia en conocimiento colectivo requiere memoria organizacional. Los aprendizajes deben incorporarse a diseños, compras, procedimientos y formación, no permanecer en la persona que resolvió una dificultad. Las bases de lecciones aprendidas son útiles si permiten buscar por tarea y condición, contienen decisiones verificadas y se depuran periódicamente. Acumular relatos sin curaduría reproduce el problema de los datos: mucho volumen y poca capacidad de acción.

1.5. Hacia una cultura preventiva basada en la confianza

La cultura preventiva se expresa en decisiones repetidas: qué ocurre cuando producción y seguridad entran en tensión, cómo responde la organización a una mala noticia, si una preocupación recibe recursos y si las reglas se aplican de modo coherente. Las declaraciones institucionales importan menos que esas experiencias. La confianza crece cuando informar un problema conduce a una respuesta justa y disminuye cuando el sistema busca culpables o promete confidencialidad que no puede garantizar.

El clima de seguridad psicosocial ofrece evidencia sobre esta relación. La revisión de alcance de Amoadu et al. (2023), que incluyó 93 estudios, encontró vínculos entre el clima psicosocial, las demandas laborales, los recursos, la calidad del liderazgo, las relaciones y resultados de salud, seguridad y desempeño. Los autores destacan el valor de políticas y prácticas que prioricen el bienestar y faciliten comunicación ascendente. Aunque los contextos estudiados son diversos, el hallazgo refuerza una idea práctica: la confianza necesita estructuras, no solo mensajes.

La introducción de IA pone a prueba esa confianza. Si el propósito no está claro, los datos se recopilan en secreto o no existe una vía para corregir errores, una herramienta preventiva puede percibirse como vigilancia. La OCDE (2023) informó preocupaciones de trabajadores sobre privacidad, pérdida de empleo y uso de datos, aun cuando las valoraciones generales de la IA en el trabajo podían ser positivas. Estudios posteriores señalan que la consulta durante la introducción de IA se asocia con mejores percepciones sobre productividad y condiciones laborales (Milanez, 2025).

La confianza tampoco significa ausencia de control. Significa que los controles son proporcionales, transparentes y orientados a riesgos reales; que se protege la información personal; que las decisiones relevantes pueden ser explicadas y revisadas, y que la responsabilidad institucional no se descarga sobre el individuo. Un sistema confiable admite incertidumbre y comunica sus límites.

La consistencia entre discurso y práctica se observa especialmente después de un incidente. Si la primera respuesta es buscar una persona responsable, los equipos aprenderán a restringir la información. Si se preservan evidencias, se

escucha a quienes participaron y se examinan condiciones técnicas y organizacionales, la investigación puede reconstruir cómo se produjo el resultado. Esto no excluye responsabilidades individuales cuando corresponden; evita decidirlas antes de comprender el sistema.

La confianza también tiene una dimensión temporal. Se construye mediante respuestas repetidas y puede perderse con una sola utilización indebida de datos sensibles. Las organizaciones necesitan compromisos verificables: registrar accesos, informar cambios de finalidad, investigar posibles abusos y aplicar consecuencias. Una política sin mecanismos de control ofrece poca protección cuando existen fuertes incentivos para utilizar la información con otros fines.

La justicia del proceso influye en la aceptación. Las personas evalúan no solo el resultado, sino si fueron escuchadas, si las reglas se aplicaron de modo consistente y si existe una vía de revisión. Una alerta algorítmica que deriva en una conversación y admite evidencia contextual produce un efecto distinto de una sanción automática. Diseñar instancias de apelación mejora la calidad de la decisión porque permite descubrir datos incorrectos y casos no previstos.

La transparencia necesita graduarse según el destinatario. La documentación completa puede ser necesaria para auditores, mientras un equipo operativo requiere una explicación breve de propósito, datos y acciones. Trabajadores y representantes deberían conocer además quién accede a la información, cuánto se conserva y qué decisiones no pueden basarse exclusivamente en ella. Estas explicaciones deben darse antes del despliegue y actualizarse cuando cambie el sistema.

1.5.1. Liderazgo, participación y responsabilidad compartida

El liderazgo preventivo se reconoce en la asignación de tiempo, autoridad y recursos. Una dirección que solicita reportes, pero no corrige problemas reiterados, enseña que informar carece de valor. Otra que suspende una tarea cuando las condiciones cambian, revisa objetivos incompatibles y explica sus decisiones convierte la seguridad en criterio operacional. ISO 45001 exige liderazgo y participación porque la prevención no puede delegarse por completo al área especializada (ISO, 2018).

La responsabilidad compartida no significa responsabilidad diluida. La alta dirección define prioridades y recursos; los mandos organizan el trabajo y responden a señales; prevención aporta método y verificación; tecnología asegura calidad, seguridad y trazabilidad; trabajadores participan y aplican controles. Los proveedores de sistemas deben documentar límites y cambios. Cada rol necesita capacidad para actuar y una ruta de escalamiento. Los comités de seguridad pueden convertirse en espacios de gobernanza de datos. Además de revisar accidentes, pueden examinar indicadores adelantados, calidad de alertas, impactos de nuevas herramientas y solicitudes de acceso. Para ello requieren información comprensible y formación suficiente. La discusión debe centrarse en patrones colectivos y evitar la exposición innecesaria de datos individuales.

Una política justa distingue error, adaptación, conducta temeraria y deficiencia del sistema. No toda desviación merece la misma respuesta. Investigar con esa diferenciación mejora la disposición a reportar y permite intervenir sobre las causas. La confidencialidad, cuando corresponda, debe acompañarse de límites claros y protección frente a represalias. Medir la cultura mediante una encuesta anual ofrece una referencia, pero no reemplaza la observación de prácticas. Conviene combinar percepciones con tiempos de respuesta, participación en análisis, calidad del cierre, repetición de hallazgos y decisiones ante conflictos. Los resultados deben segmentarse con prudencia para detectar desigualdades sin identificar indebidamente a personas o grupos pequeños.

1.5.2. Tecnología con propósito humano

Una tecnología con propósito humano empieza por un problema preventivo, no por una herramienta disponible. La organización debe describir la exposición que pretende reducir, la decisión que necesita mejorar y el resultado esperado. Después evalúa alternativas siguiendo la jerarquía de controles. Si es posible eliminar una tarea peligrosa, no resulta razonable instalar un dispositivo que solo avise al trabajador cada vez que se expone. El diseño centrado en las personas incorpora a usuarios y afectados desde el inicio. EU-OSHA (2025a) propone sistemas inclusivos, comprensibles, confiables e integrados en los marcos preventivos existentes. Esto se traduce en interfaces claras, alarmas

accionables, pruebas bajo condiciones reales, accesibilidad, capacitación y canales de retroalimentación. También exige separar, cuando sea posible, datos preventivos de métricas de productividad.

La supervisión humana debe ser efectiva. No basta con colocar a una persona al final de un proceso si carece de tiempo, información o autoridad para contradecir el algoritmo. Quien supervisa necesita conocer la incertidumbre, revisar casos relevantes y documentar cuándo acepta o rechaza una recomendación. La automatización sesgada hacia la confirmación —seguir la salida porque "lo dijo el sistema"— es especialmente peligrosa en tareas de alta consecuencia.

- Un programa responsable de analítica preventiva puede organizarse mediante siete preguntas:
- ¿Qué peligro, exposición o decisión se busca mejorar?
- ¿Qué datos son realmente necesarios y qué colectivos podrían quedar subrepresentados?
- ¿Cómo se validará el sistema en condiciones reales y qué nivel de error es aceptable?
- ¿Quién recibe la alerta, qué acción puede ejecutar y en cuánto tiempo?
- ¿Cómo pueden trabajadores y representantes conocer, cuestionar y corregir la información?
- ¿Qué medidas protegen privacidad, seguridad y usos compatibles con la finalidad original?
- ¿Cómo se comprobará que la herramienta reduce el riesgo sin crear daños nuevos?

Estas preguntas conectan la gestión preventiva con los principios de gobernanza, mapeo, medición y gestión del NIST (Tabassi, 2023). También obligan a evaluar resultados más allá de la precisión del modelo. Una implementación exitosa debería mejorar controles, acortar respuestas o reducir exposiciones sin aumentar presión, discriminación ni vigilancia desproporcionada.

La rendición de cuentas requiere inventario de sistemas, responsables, versiones, fuentes de datos y evaluaciones. Los modelos cambian cuando

cambia el trabajo; su desempeño puede deteriorarse por nuevas máquinas, turnos, poblaciones o procedimientos. La revisión periódica debe buscar deriva, sesgo y efectos no previstos. Cuando el riesgo supera el beneficio, debe existir una decisión clara para modificar o retirar la herramienta. La evaluación puede organizarse en cuatro capas. La primera examina desempeño técnico: precisión, disponibilidad y robustez. La segunda considera el proceso: tiempo de respuesta, carga y cumplimiento de acciones. La tercera observa resultados de exposición y salud, evitando atribuir causalidad sin diseño adecuado. La cuarta revisa consecuencias distributivas: quién recibe beneficios, quién soporta vigilancia y si algunos grupos acumulan errores. Esta mirada evita declarar éxito porque una sola métrica mejoró.

La innovación preventiva debería conservar reversibilidad. Los pilotos limitados, las revisiones independientes y los puntos de decisión permiten aprender sin comprometer a toda la organización. La posibilidad de volver a un modo seguro cuando el sistema falla es tan importante como la capacidad de escalarlo. Una herramienta cuyo retiro resulta operacionalmente imposible crea dependencia y reduce la autonomía institucional.

En América Latina, el propósito humano incluye fortalecer capacidades y soberanía sobre decisiones. Contratos claros, documentación en español, transferencia de conocimiento y posibilidad de exportar datos reducen dependencia del proveedor. La cooperación entre empresas, universidades, autoridades y organizaciones de trabajadores puede generar criterios y conjuntos de datos pertinentes para realidades regionales, siempre bajo reglas éticas y de protección. Prevenir en un mundo laboral cambiante demanda combinar memoria y anticipación. Los accidentes y enfermedades siguen siendo fuentes esenciales de aprendizaje, pero no bastan para describir el estado actual de un sistema. Los indicadores adelantados, los reportes, la vigilancia de exposiciones y la experiencia del trabajador amplían la capacidad de reconocer degradaciones antes del daño. La IA y el Big Data pueden integrar esas señales y apoyar decisiones más oportunas, aunque su valor depende de datos adecuados, validación, contexto y acciones concretas.

La transformación digital introduce una responsabilidad adicional: cuidar también significa gobernar la tecnología. Privacidad, explicabilidad, ciberseguridad, equidad y supervisión humana forman parte de la prevención porque una herramienta mal diseñada puede crear riesgos mientras intenta controlar otros. La gestión no debería preguntarse únicamente si un modelo predice, sino qué decisión modifica, quién responde, a quién puede perjudicar y cómo se comprueba su aporte.

La experiencia de quienes realizan el trabajo enlaza los datos con la realidad operacional. Sin participación, las señales pierden contexto; sin confianza, dejan de comunicarse. Liderazgo, consulta y una respuesta organizacional justa convierten la información en aprendizaje. De este modo, la innovación deja de ser una capa tecnológica y se integra en una cultura preventiva capaz de observar, dialogar y actuar antes de que el daño haga evidente lo que ya estaba ocurriendo.

Figura 1.

Fundamentos de la Transformación Digital

Capítulo II: Datos y tecnologías para anticiparse al riesgo

Datos y tecnologías para anticiparse al riesgo

Anticiparse a un riesgo laboral exige observar señales que, durante mucho tiempo, permanecieron dispersas: una variación de temperatura, el aumento gradual del ruido, una postura sostenida, una alarma recurrente, una desviación de proceso o una sucesión de incidentes menores. Por separado, cada registro puede parecer poco concluyente. Cuando se integra con su contexto —tarea, lugar, turno, equipo, exposición y decisión adoptada— empieza a describir cómo se forma una condición peligrosa. La transformación digital aplicada a la seguridad y salud en el trabajo (SST) consiste, en buena medida, en convertir esas huellas en conocimiento útil antes de que el daño ocurra.

La tecnología amplía la capacidad de observación, pero no elimina las preguntas básicas de la prevención. ¿Qué se mide y con qué propósito? ¿A quién representa el dato y a quién deja fuera? ¿Qué error admite el sensor? ¿Quién interpreta una alerta? ¿Qué acción está autorizada y en cuánto tiempo debe ejecutarse? Un sistema técnicamente sofisticado puede producir una falsa sensación de control si no responde con claridad a estas cuestiones. Ezerins et al. (2022) sostienen que la analítica de seguridad depende tanto de la preparación organizacional como de los métodos estadísticos: requiere datos disponibles, competencias, infraestructura, cultura y capacidad para traducir resultados en intervenciones.

Este capítulo examina la cadena completa que va desde la captura hasta la actuación. Primero aborda la integración y calidad de la información; después analiza sensores ambientales, dispositivos portátiles y Big Data. A continuación estudia los modelos de inteligencia artificial (IA), las alertas tempranas y la supervisión humana. Finalmente, revisa la visualización, la realidad virtual (RV) y los gemelos digitales como medios para comprender, ensayar y decidir sin exponer innecesariamente a las personas. La idea que articula el recorrido es sencilla: el valor preventivo no reside en acumular datos, sino en mejorar decisiones concretas con evidencia trazable, oportuna y proporcional al riesgo.

2.1. Del dato aislado a la inteligencia preventiva

Un registro adquiere sentido preventivo cuando puede relacionarse con una pregunta operacional. El valor de 87 dB(A), por ejemplo, no describe por sí solo la exposición de una persona: hacen falta duración, ubicación, incertidumbre del instrumento, condiciones de la tarea, uso efectivo de controles y población expuesta. Algo similar ocurre con una fotografía de una postura, la frecuencia cardiaca o el número mensual de incidentes. La cifra aislada puede activar una revisión, pero la inteligencia preventiva aparece cuando diversas fuentes permiten reconstruir condiciones, tendencias y posibles causas.

Esta transformación admite, al menos, cuatro niveles. El nivel descriptivo responde qué ocurrió: cuántas alarmas se activaron, dónde y durante qué actividad. El diagnóstico busca relaciones plausibles: qué combinación de carga, mantenimiento, organización del turno o condición ambiental acompañó el evento. El nivel predictivo estima la probabilidad de una situación futura bajo condiciones definidas. El prescriptivo compara opciones de control y apoya una decisión. La progresión no es automática; una organización puede disponer de abundantes tableros descriptivos y carecer de la calidad o madurez necesarias para predecir de manera confiable.

Foreman et al. (2023) advierten que la analítica de seguridad a escala de establecimiento enfrenta problemas recurrentes: definiciones inconsistentes, subregistro, bases pequeñas, indicadores rezagados y escasa cultura de datos. Los accidentes graves son afortunadamente poco frecuentes, pero esa baja frecuencia dificulta entrenar modelos y evaluar su desempeño. Además, registrar solo lesiones consolida una mirada retrospectiva. Las observaciones de trabajo, cuasi accidentes, fallas de barreras, exposiciones, órdenes de mantenimiento y cambios del proceso aportan indicadores adelantados; ninguno debería confundirse, sin embargo, con una medida perfecta del riesgo.

La inteligencia preventiva combina tres clases de evidencia. La primera proviene del proceso: parámetros de máquinas, estados de barreras, velocidad, presión, temperatura y secuencia de operaciones. La segunda describe el ambiente y la exposición: ruido, gases, partículas, iluminación, vibración o estrés térmico. La tercera recoge la experiencia humana: reportes, síntomas, observaciones,

percepción de fatiga y conocimiento práctico. Si el sistema privilegia únicamente lo que un sensor puede medir, puede volver invisibles riesgos psicosociales, conflictos de objetivos, procedimientos inviables o estrategias informales que mantienen segura la operación.

Una arquitectura útil conserva el vínculo entre señal y contexto. El evento debe incluir hora, ubicación, fuente, unidad, calibración, tarea, equipo y reglas de tratamiento; los datos personales requieren controles adicionales de necesidad, acceso y conservación. Después se validan, armonizan y almacenan los registros, se aplican reglas o modelos y se presenta un resultado comprensible. La última etapa es decisiva: asignar responsable, acción, plazo y mecanismo de cierre. Una alerta sin ruta de respuesta no constituye prevención, sino ruido organizacional.

2.1.1. Capturar, integrar y comprender la información

La captura comienza con una definición operacional. Antes de instalar un dispositivo conviene formular el peligro, la población, la decisión que se busca apoyar y el nivel de resolución necesario. Medir cada segundo puede ser pertinente para detectar un pico de gas, pero innecesario para algunas variables administrativas. Una frecuencia excesiva aumenta costos, tráfico, almacenamiento y falsos positivos; una frecuencia baja puede ocultar transitorios críticos. El diseño debe corresponder a la dinámica del fenómeno, no a la máxima capacidad del equipo.

Las fuentes habituales incluyen sistemas de gestión de SST, mantenimiento, producción, recursos humanos, vigilancia de la salud, inspecciones, permisos de trabajo, sensores fijos, equipos móviles y dispositivos portátiles. Integrarlas exige vocabularios comunes. Si “caída”, “resbalón” y “pérdida de equilibrio” se registran sin reglas, los análisis pueden fragmentar un mismo mecanismo. También se necesitan identificadores coherentes para áreas, activos y tareas, así como sellos temporales sincronizados. La interoperabilidad no es un asunto puramente informático: expresa acuerdos sobre qué significa cada campo y quién responde por su calidad.

El proceso de integración suele adoptar una secuencia de extracción, transformación y carga o un flujo continuo de eventos. Durante la transformación

se corrigen formatos, unidades y zonas horarias; se gestionan duplicados; se documentan valores ausentes, y se vinculan tablas mediante claves. Conviene conservar los datos originales y registrar cada cambio para asegurar trazabilidad. Cuando una variable es derivada —por ejemplo, una categoría de exposición construida desde varias mediciones— deben quedar visibles su fórmula, versión y supuestos.

Comprender la información requiere metadatos. Un valor sin procedencia, unidad o intervalo de medición puede ser inutilizable. También importa distinguir entre persona, tarea y ambiente: la concentración ambiental no equivale necesariamente a la dosis individual, y una señal biométrica no identifica por sí sola la causa laboral. La interpretación debe considerar factores de confusión, condiciones de referencia y límites del instrumento. En vigilancia ocupacional, la cercanía temporal entre una exposición y un cambio fisiológico puede orientar una investigación, pero no prueba causalidad.

La gobernanza define qué datos se recogen, para qué fines, durante cuánto tiempo y quién puede utilizarlos. La Agencia Europea para la Seguridad y la Salud en el Trabajo ha señalado que los sistemas digitales inteligentes deben diseñarse con participación de trabajadores, transparencia y protección de datos, evitando que el monitoreo preventivo se convierta en vigilancia desproporcionada (European Agency for Safety and Health at Work [EU-OSHA], 2025). Este principio es especialmente relevante en dispositivos que generan información continua o identificable.

La integración también debe preservar el significado temporal. Un evento de exposición puede preceder a un síntoma por minutos, horas o años, mientras que una falla operacional suele desarrollarse mediante señales de degradación. Alinear registros solo por fecha diaria puede ocultar secuencias breves; exigir coincidencia exacta puede perder relaciones cuando los relojes difieren. El criterio de enlace debe basarse en el fenómeno y quedar documentado. En análisis longitudinales, los cambios de puesto, turno y equipo requieren fechas de inicio y fin para no atribuir una exposición a quien ya no realizaba la tarea.

Otro componente es la observabilidad del propio sistema. Además de la variable preventiva, se registran batería, conexión, versión, calibración y tasa de pérdida.

Estos datos permiten distinguir entre ausencia de peligro y ausencia de medición. Un panel que muestra “sin alarmas” durante una caída de comunicaciones ofrece una conclusión peligrosa; debería mostrar “estado desconocido” y activar el procedimiento correspondiente. La calidad técnica se convierte así en una barrera que también necesita vigilancia.

Una práctica sólida consiste en separar los usos. Los datos necesarios para activar una protección inmediata no tienen por qué alimentar automáticamente evaluaciones disciplinarias o de productividad. La limitación de finalidad reduce riesgos de abuso y favorece la confianza, condición sin la cual las personas pueden retirar dispositivos, alterar conductas o dejar de reportar. También deben definirse niveles de agregación: muchas decisiones de prevención pueden tomarse por zona, tarea o turno sin identificar a cada trabajador.

2.1.2. La calidad del dato y sus consecuencias humanas

La calidad comprende exactitud, completitud, consistencia, oportunidad, validez y representatividad. Cada dimensión puede fallar de manera distinta. Un sensor descalibrado produce valores precisos en apariencia, pero alejados de la exposición real; un formulario incompleto elimina contexto; una taxonomía que cambia entre plantas impide comparar; una alerta tardía llega después de la ventana de intervención. La consecuencia no es solo estadística. Un dato defectuoso puede enviar a una persona a una zona peligrosa, ocultar una exposición o concentrar recursos donde el riesgo es menor.

Los valores ausentes merecen atención específica. No siempre faltan al azar: un dispositivo puede perder conexión en un túnel, una persona puede retirar un wearable cuando incomoda o un supervisor puede omitir reportes en periodos de presión productiva. Imputar automáticamente esos vacíos puede borrar justamente las condiciones que explican el riesgo. Antes de completar registros conviene estudiar el mecanismo de ausencia y realizar análisis de sensibilidad. Cuando la incertidumbre es alta, el resultado debe presentarse como rango o nivel de confianza, no como cifra exacta.

La representatividad plantea otra dificultad. Los datos históricos reflejan quién fue contratado, qué tareas se midieron y qué incidentes se documentaron. Si una base contiene principalmente trabajadores varones de una planta, el modelo

puede funcionar peor en mujeres, contratistas o instalaciones con otros procesos. Fisher et al. (2023) identifican que la IA puede apoyar la equidad en SST, pero también reproducir desigualdades cuando los conjuntos de datos o las decisiones automatizadas excluyen a ciertos grupos. Auditar desempeño por subpoblación, turno, ocupación y contexto es parte del control preventivo.

Los errores de etiqueta afectan los modelos supervisados. Clasificar un incidente como “acto inseguro” cuando existieron fallas de diseño, mantenimiento o supervisión enseña al algoritmo una explicación sesgada. El sistema podría terminar señalando características individuales en lugar de condiciones controlables. Por ello, la codificación requiere criterios explícitos, revisión por más de un especialista en casos complejos y mecanismos para corregir categorías. La taxonomía debe representar mecanismos de daño, exposiciones y barreras, no buscar culpables.

También existe una dimensión temporal. Los procesos cambian, se sustituyen equipos, aparecen materiales y se modifican procedimientos. Un modelo entrenado con la operación de 2022 puede perder validez en 2026 aunque el software continúe funcionando. Este desplazamiento —conocido como deriva de datos o de concepto— exige monitorear distribuciones, tasas de error y cambios del proceso. La recalibración no debe realizarse a ciegas: una reducción de alertas podría indicar mejora real, deterioro del sensor o adaptación de las conductas para evitar el monitoreo.

La respuesta organizacional frente al error debería ser proporcional. En un tablero exploratorio puede aceptarse cierta latencia; en una alarma de atmósfera peligrosa se requieren validación, redundancia y conducta segura ante fallas. Los falsos negativos dejan pasar condiciones peligrosas, mientras que los falsos positivos interrumpen tareas y, si son frecuentes, generan fatiga de alarmas. No existe un umbral universal: debe elegirse considerando gravedad, reversibilidad, tiempo disponible y capacidad de verificación humana.

2.2. Sensores que observan el entorno laboral

Los sensores convierten propiedades físicas, químicas o biológicas en señales analizables. Pueden ser fijos, móviles, integrados en maquinaria, instalados en vehículos o portados por trabajadores. Su ventaja principal es ampliar cobertura

y continuidad frente a las mediciones puntuales; su limitación es que toda señal depende del lugar, la tecnología, la calibración y el contexto. La presencia de un sensor no equivale a una evaluación de riesgo completa.

Un sistema típico combina el elemento de detección, acondicionamiento de señal, procesamiento, comunicación y plataforma de análisis. En el borde de la red, algunos dispositivos filtran o interpretan datos antes de transmitirlos. Ese procesamiento local reduce latencia y permite actuar cuando la conectividad falla; también obliga a gestionar versiones y ciberseguridad en múltiples equipos. La nube facilita integración y cómputo, aunque incrementa la dependencia de comunicaciones y exige definir dónde se almacenan los datos.

La selección debe considerar rango, sensibilidad, selectividad, tiempo de respuesta, deriva, robustez, autonomía y facilidad de calibración. Un instrumento adecuado en laboratorio puede fallar ante polvo, humedad, vibración o interferencias electromagnéticas. La validación en condiciones reales, comparada con un método de referencia, evita desplegar soluciones que funcionan solo en demostraciones. También importa el mantenimiento: filtros saturados, baterías degradadas y firmware desactualizado pueden modificar la respuesta sin producir una falla visible.

La conectividad incorpora riesgos propios. La pérdida de paquetes, los relojes desincronizados o una red congestionada pueden fragmentar series temporales. Una arquitectura segura autentica dispositivos, cifra comunicaciones, controla actualizaciones y limita privilegios. Para funciones críticas se necesitan modos degradados seguros: si la plataforma central no responde, el control local debe conservar la alarma o llevar el proceso a una condición estable.

2.2.1. Monitoreo ambiental y operacional

El monitoreo ambiental digital puede abarcar gases, partículas, ruido, vibración, temperatura, humedad, radiación e iluminación. Su utilidad aumenta cuando la medición se vincula con ubicación y actividad. Una red de sensores de partículas permite reconocer gradientes espaciales; una serie de ruido asociada a estados de máquina ayuda a identificar la fase que genera picos; la combinación de temperatura, humedad, carga metabólica y vestimenta puede apoyar la

evaluación del estrés térmico. El resultado debe contrastarse con métodos higiénicos y límites aplicables, no reemplazarlos de forma indiscriminada.

En atmósferas peligrosas, la ubicación del detector determina lo que puede observar. La densidad del gas, los flujos de ventilación, las barreras físicas y los puntos de fuga influyen en la lectura. Un mapa con baja concentración en un lugar no garantiza seguridad en otro. Los sensores portátiles añaden proximidad a la persona, mientras los fijos ofrecen continuidad y estabilidad; combinarlos suele ser más informativo que elegir uno solo.

El monitoreo operacional registra condiciones de equipos y procesos: temperatura de rodamientos, vibración, corriente, presión, velocidad, proximidad, apertura de resguardos o estado de válvulas. Estas variables permiten detectar degradación antes de una falla. La conexión con mantenimiento predictivo puede reducir la probabilidad de roturas, escapes o movimientos inesperados, pero una predicción de condición mecánica no sustituye bloqueo, resguardos ni inspecciones. La jerarquía de controles sigue siendo la referencia para decidir: la información debe favorecer eliminación, sustitución o controles de ingeniería antes de depender de advertencias.

La visión por computador añade cámaras y modelos capaces de reconocer proximidad, presencia en zonas restringidas o uso de equipos de protección. Tiene ventajas de cobertura y riesgos significativos de privacidad, sesgo y mala interpretación. La oclusión, iluminación, ángulo y diversidad de prendas afectan el desempeño; además, detectar un casco no demuestra que el sistema de trabajo sea seguro. Su aplicación debería limitarse a finalidades definidas, evaluar errores por contexto y ofrecer mecanismos de revisión.

Las alarmas ambientales requieren reglas de escalamiento. Un umbral puede generar aviso local, reducción automática del proceso, evacuación o verificación instrumental, según la gravedad. Las tendencias también importan: una concentración aún inferior al límite, pero en ascenso rápido, puede justificar acción. La lógica y los retardos deben documentarse para evitar que el filtrado suprima un pico crítico. Cada alarma necesita prueba periódica de extremo a extremo, desde el detector hasta la respuesta humana u operacional.

2.2.2. Dispositivos portátiles y variables biométricas

Los dispositivos portátiles —relojes, bandas, chalecos, cascos, plantillas, parches y sensores textiles— acercan la medición a la experiencia individual. Pueden registrar movimiento, postura, localización, frecuencia cardiaca, temperatura cutánea, actividad muscular o indicadores indirectos de fatiga. La revisión sistemática de Mendes et al. (2026), basada en 60 estudios, muestra una expansión de estas tecnologías en SST y propone una implementación centrada en la persona. La evidencia, sin embargo, es heterogénea y muchos prototipos no han sido evaluados durante periodos prolongados.

En ergonomía, las unidades inerciales permiten estimar ángulos, repetición y duración de posturas. Son útiles para identificar segmentos de tarea que merecen rediseño, siempre que el modelo se valide para el movimiento, cuerpo y colocación concretos. Un aviso vibratorio puede ayudar a corregir temporalmente una postura, pero desplaza la intervención hacia el individuo si la estación, herramienta o ritmo permanecen sin cambios. El propósito debería ser localizar oportunidades de rediseño, no entrenar al cuerpo para tolerar una tarea deficiente.

Las variables fisiológicas son sensibles, pero poco específicas. Una frecuencia cardiaca elevada puede relacionarse con esfuerzo, calor, estrés, medicación o condición física. La temperatura cutánea no equivale a temperatura corporal central; los algoritmos propietarios pueden ocultar cómo se produce un “índice de fatiga”. Por eso, los indicadores deben interpretarse como señales que requieren contexto y, cuando corresponda, valoración profesional. No deberían utilizarse para diagnosticar enfermedades ni declarar aptitud laboral sin un marco clínico y legal adecuado.

La aceptabilidad depende de comodidad, autonomía y confianza. Peso, presión, calor, duración de batería y falsas alarmas modifican el uso real. La participación temprana permite conocer si el dispositivo interfiere con equipos de protección, movimientos o relaciones de trabajo. EU-OSHA (2023) subraya que la implantación debe incluir información, consulta, formación, mantenimiento y evaluación continua. Un piloto no debería limitarse a medir precisión; también

debe estudiar carga de uso, comprensión, consecuencias imprevistas y distribución de beneficios.

La privacidad exige minimización. Si basta una alerta local para indicar proximidad, quizá no sea necesario conservar la trayectoria completa. Si el análisis puede hacerse con un identificador seudónimo o datos agregados, registrar nombres aumenta riesgo sin añadir valor preventivo. Deben definirse acceso, retención, portabilidad, tratamiento de hallazgos incidentales y prohibición de usos incompatibles. El trabajador necesita saber qué mide el dispositivo, qué no puede inferir y cómo cuestionar un resultado.

2.3. Big Data: descubrir patrones donde antes había incertidumbre

Big Data describe entornos en los que volumen, velocidad, variedad y complejidad exceden los métodos convencionales. En SST, el concepto cobra sentido al integrar series de sensores, narrativas de incidentes, mantenimiento, producción, imágenes, clima, turnos y observaciones. No toda organización necesita una infraestructura masiva; a menudo, mejorar un conjunto pequeño y relevante produce más valor que acumular datos sin propósito. La escala debe justificarse por la pregunta preventiva.

La variedad permite observar interacciones que los registros aislados ocultan. Un aumento de cuasi accidentes puede coincidir con horas extra, cambios de contratistas, presión de producción o degradación de un activo. La analítica temporal identifica secuencias; el análisis espacial localiza concentraciones; el procesamiento de lenguaje natural organiza narrativas; y las redes relacionan personas, equipos y tareas. Estos patrones orientan hipótesis, no prueban causas. Una asociación histórica puede surgir por registro diferencial, estacionalidad o variables no medidas.

Ezerins et al. (2022) proponen evaluar la preparación para la analítica mediante dimensiones organizacionales y técnicas. Esta perspectiva evita comprar plataformas antes de resolver definiciones, responsabilidades y competencias. El trabajo preparatorio incluye inventariar fuentes, mapear flujos, definir un diccionario, evaluar sesgos y acordar decisiones. También requiere personal

capaz de conversar entre higiene, ergonomía, operaciones, ciencia de datos, privacidad y representación laboral.

La arquitectura puede incluir un lago de datos para registros diversos, un almacén estructurado para indicadores y flujos en tiempo real para eventos críticos. La separación entre capas permite conservar datos brutos y ofrecer conjuntos curados. Un catálogo documenta procedencia, calidad y permisos. Los controles de acceso deben seguir el principio de mínimo privilegio, y los registros de auditoría deben mostrar quién consultó o modificó información. La disponibilidad sin gobernanza multiplica copias y contradicciones.

El análisis de narrativas merece cautela. Los modelos pueden agrupar textos o extraer mecanismos de lesión, pero heredan la calidad del reporte. Si el lenguaje culpabiliza a la persona o excluye condiciones organizacionales, el patrón aprendido será incompleto. Una muestra manual estratificada permite comprobar precisión y descubrir categorías emergentes. Los resultados deben presentarse con ejemplos anonimizados y tasas de error, no como clasificación incuestionable.

Big Data también facilita evaluar intervenciones. Las series antes y después de un control pueden revelar cambios, aunque se deben considerar tendencias, estacionalidad y modificaciones simultáneas. Cuando no es posible un ensayo, los diseños cuasiexperimentales y las comparaciones entre áreas pueden fortalecer inferencias. El indicador final no debería ser solo el uso de la plataforma, sino la reducción de exposición, el funcionamiento de barreras y, cuando la evidencia lo permita, los resultados de salud.

La analítica federada constituye una opción cuando varias instalaciones necesitan aprender sin centralizar todos los datos personales. Los modelos se entrenan localmente y comparten parámetros o resultados agregados; esto puede reducir transferencias, pero no garantiza privacidad por sí mismo. También demanda definiciones compatibles y control de calidad entre sedes. Para organizaciones pequeñas, una alternativa más sencilla es compartir taxonomías y conjuntos anonimizados bajo acuerdos de gobernanza. La elección depende del riesgo, el volumen y la capacidad técnica.

El costo total suele quedar subestimado. A licencias y sensores se añaden conectividad, limpieza, calibración, ciberseguridad, soporte, formación y tiempo de especialistas. Una prueba de concepto puede funcionar con atención intensiva que luego desaparece. Antes de escalar conviene estimar costos de ciclo de vida y criterios de salida: si la herramienta no alcanza desempeño, aceptación o impacto acordados, debe modificarse o retirarse. Mantener un sistema sin utilidad comprobada consume recursos y puede desplazar controles materiales.

En América Latina, las oportunidades conviven con fragmentación tecnológica, desigualdad de conectividad y heterogeneidad regulatoria. La publicación *Salud Digital 4.0* aporta un marco regional sobre interoperabilidad, analítica predictiva, privacidad y trazabilidad en entornos sanitarios (Rodríguez-Lindao et al., 2026). Aunque su campo no es idéntico a la SST, sus problemas de integración y gobernanza son transferibles con prudencia: la transformación no puede depender de sistemas costosos que excluyan pequeñas organizaciones o trabajadores informales. Soluciones escalables, estándares abiertos y capacidad local resultan más sostenibles que plataformas cerradas sin soporte.

2.4. Inteligencia artificial para reconocer y anticipar riesgos

La IA reúne métodos capaces de identificar patrones, clasificar señales, estimar probabilidades o generar recomendaciones. En prevención se aplica a imágenes, series temporales, texto y datos tabulares. Sus usos incluyen detectar equipos de protección, reconocer caídas, pronosticar incidentes, estimar exposición y priorizar inspecciones. El término no debería emplearse como sinónimo de automatización: una regla fija de umbral puede ser suficiente, más explicable y segura que un modelo complejo.

La revisión de La Torre et al. (2026) describe aplicaciones crecientes de IA en SST, junto con desafíos éticos, sociales y operacionales. Jetha et al. (2025), al preguntar si las herramientas con IA producen un impacto medible sobre lesiones o enfermedades, encontraron que la evidencia de resultados finales sigue siendo limitada. Esta diferencia entre capacidad técnica e impacto preventivo es central. Un modelo puede clasificar imágenes con alta precisión y no reducir accidentes si las alertas no llegan, se ignoran o sustituyen controles más eficaces.

El ciclo de vida empieza con el problema, no con el algoritmo. Se define la decisión, el horizonte y el costo de errores; después se seleccionan datos, se separan conjuntos de entrenamiento y prueba y se establece una línea base. La validación debe evitar fuga de información: registros del mismo trabajador, equipo o evento no deberían aparecer en entrenamiento y prueba si eso infla artificialmente el desempeño. La validación externa en otro periodo o instalación ofrece una prueba más realista.

Las métricas deben corresponder al uso. La exactitud puede ser engañosa cuando los eventos peligrosos son raros. Sensibilidad, especificidad, valor predictivo, calibración y curvas precisión–exhaustividad aportan información complementaria. En una alerta crítica puede priorizarse sensibilidad, pero el aumento de falsos positivos debe ser operacionalmente tolerable. La calibración indica si, entre casos con riesgo estimado de 20 %, aproximadamente una quinta parte presenta el evento; sin ella, una probabilidad aparente puede no ser útil para decidir.

La explicabilidad tiene niveles. Un técnico puede necesitar saber qué variable activó la alerta; un responsable de SST, cómo se comporta el modelo por área; un trabajador, qué datos se usaron y cómo solicitar revisión. Una explicación post hoc no corrige un modelo sesgado, pero puede revelar dependencias impropias. Para decisiones de alto impacto conviene preferir modelos interpretables cuando su desempeño sea suficiente y mantener documentación de datos, versiones, limitaciones y usos prohibidos.

2.4.1. Modelos predictivos aplicados a la prevención

Los modelos predictivos estiman un resultado futuro o no observado a partir de variables disponibles. Pueden utilizar regresión, árboles, bosques aleatorios, máquinas de soporte vectorial, redes neuronales o métodos de series temporales. La revisión de Armenteros-Cosme et al. (2025) muestra que la literatura de modelado predictivo en seguridad laboral se concentra especialmente en construcción y combina datos de incidentes, comportamiento, ambiente y operación. La diversidad metodológica dificulta comparar resultados y refuerza la necesidad de validación contextual.

Definir el resultado es una decisión conceptual. Predecir lesiones registradas puede reproducir el subregistro; predecir cuasi accidentes depende de la cultura de reporte; estimar exposición requiere mediciones adecuadas. En ocasiones es preferible modelar el fallo de una barrera o la entrada en una condición peligrosa, porque ofrece una acción más directa. El horizonte también cambia la intervención: una alerta de segundos puede detener una máquina, mientras un pronóstico mensual orienta mantenimiento o capacitación.

Las variables deben estar disponibles antes de la decisión. Incluir información registrada después del incidente produce un modelo aparentemente excelente, pero inútil en operación. También conviene limitar variables proxy que reflejan grupos protegidos o desigualdades históricas. El turno, por ejemplo, puede capturar diferencias de dotación o mantenimiento; atribuir el riesgo a las personas del turno sin investigar esas condiciones desviaría la prevención.

El entrenamiento debe gestionar el desequilibrio de clases. Técnicas de ponderación o remuestreo pueden ayudar, pero no sustituyen una evaluación con prevalencia real. La validación temporal es especialmente importante: entrenar con años anteriores y probar en un periodo posterior imita el uso futuro. Cuando el proceso cambia, el modelo necesita revalidación. Un umbral aprobado para una planta no debería trasladarse a otra sin comprobar desempeño y capacidad de respuesta.

Un modelo predictivo útil termina en una intervención especificada. Si identifica mayor probabilidad de exposición durante cierta operación, la respuesta puede ser rediseñar ventilación, reprogramar mantenimiento o detener una tarea. La predicción no debe utilizarse para seleccionar a quienes “toleran mejor” el riesgo. La SST busca controlar la fuente y el sistema de trabajo, no adaptar la fuerza laboral a condiciones dañinas.

2.4.2. Alertas tempranas y apoyo a la toma de decisiones

Una alerta temprana traduce señales en una solicitud de atención antes de que la situación alcance consecuencias graves. Su diseño combina umbral, ventana temporal, severidad, destinatario y acción. Puede basarse en una regla transparente, un cambio respecto de la línea base o una probabilidad estimada.

La complejidad solo se justifica si mejora detección, oportunidad o discriminación de manera comprobable.

Las alertas deberían clasificarse por criticidad. Un aviso informativo puede incluirse en un tablero; una advertencia exige verificación; una alarma crítica activa protección inmediata. Mezclar todos los eventos en el mismo canal produce saturación. El mensaje debe indicar qué se detectó, dónde, con qué confianza, qué conducta provisional adoptar y quién confirma el cierre. Mostrar solo un color rojo obliga a reconstruir el significado bajo presión.

La fatiga de alarmas surge cuando el volumen supera la atención o muchas señales no requieren acción. Reducirla implica revisar umbrales, agrupar eventos relacionados, suprimir duplicados y retirar reglas sin valor. No debe confundirse optimización con ocultamiento: cada cambio necesita evaluar si aumenta falsos negativos. Los datos de reconocimiento, tiempo de respuesta y resultado de la intervención permiten ajustar el sistema.

El apoyo a decisiones puede ordenar inspecciones, presentar escenarios o recomendar controles. La recomendación debe incluir evidencia y alternativas, no solo una salida. Un responsable puede aceptar, modificar o rechazar la sugerencia dejando una razón. Ese registro favorece aprendizaje y auditoría, siempre que no se convierta en burocracia defensiva. Las discrepancias recurrentes pueden indicar que el modelo desconoce restricciones operacionales o que la formación es insuficiente.

La automatización de una acción requiere una evaluación de seguridad funcional. Detener un equipo puede evitar una colisión, pero también crear otro peligro si el estado resultante no es seguro. Por eso se analizan fallas, redundancia, latencia y recuperación. Las funciones críticas deben probarse en condiciones normales, degradadas y de emergencia; además, la persona debe comprender cuándo puede intervenir y qué ocurre si el sistema no está disponible.

2.4.3. La necesaria supervisión del criterio humano

La supervisión humana no consiste en colocar una firma al final de una decisión automática. Requiere autoridad, tiempo, información y competencia para

cuestionar el resultado. Si la organización sanciona toda discrepancia o presenta el modelo como infalible, la revisión se vuelve simbólica. El criterio profesional debe poder examinar datos, contexto, alternativas y consecuencias.

El sesgo de automatización lleva a aceptar recomendaciones por provenir de una máquina; la aversión algorítmica produce el efecto contrario tras observar un error. Ambos extremos se controlan con formación, diseño transparente y práctica. Las interfaces deben evitar probabilidades con precisión ficticia y distinguir entre dato observado, inferencia y recomendación. Un intervalo o nivel de incertidumbre suele ser más honesto que un 83,47 % sin contexto.

El marco de gestión de riesgos de IA del National Institute of Standards and Technology organiza la gobernanza en funciones de gobernar, mapear, medir y gestionar (Tabassi, 2023). Aplicado a SST, esto implica asignar responsables, comprender el contexto, evaluar desempeño y riesgos y adoptar controles durante todo el ciclo de vida. El monitoreo debe incluir seguridad, privacidad, equidad, explicabilidad y robustez, no solo precisión.

El-Helaly (2024) resume beneficios potenciales y desventajas de la IA ocupacional, entre ellas privacidad, sesgo, dependencia y desplazamiento de responsabilidades. La organización conserva el deber de proteger incluso cuando un proveedor opera el algoritmo. Los contratos deberían permitir auditoría, notificación de cambios, acceso a documentación, gestión de incidentes y eliminación segura de datos. Un modelo actualizado silenciosamente puede alterar umbrales sin que el usuario comprenda por qué.

La participación de los trabajadores aporta conocimiento difícil de capturar. Ellos pueden explicar por qué una alerta aparece durante una maniobra segura, qué dispositivo interfiere con la tarea o qué indicador incentiva ocultamiento. La participación no equivale a informar después del despliegue; comprende diseño, piloto, evaluación y revisión. También debe existir un canal de impugnación cuando una inferencia afecte asignación de tareas, vigilancia de la salud o empleo.

Un comité de gobernanza puede reunir SST, operaciones, tecnología, protección de datos, medicina del trabajo y representación laboral. Su función no es aprobar cada resultado, sino definir usos permitidos, revisar desempeño, investigar

daños y decidir cambios. Las reuniones deberían apoyarse en un registro de modelos que incluya propietario, versión, datos, propósito, métricas, grupos evaluados, incidentes y fecha de revisión. Esta documentación evita que una herramienta siga operando cuando ya nadie conoce su origen o limitaciones.

La retirada segura merece el mismo cuidado que el despliegue. Si una alerta se integra a procedimientos, eliminarla sin transición crea dependencia no reconocida. El plan debe establecer controles alternativos, exportación de registros, eliminación verificable y comunicación. También se examina si la automatización debilitó competencias: operadores que dejaron de practicar diagnóstico manual pueden necesitar reentrenamiento antes de volver a un modo convencional.

Finalmente, algunas decisiones no deberían automatizarse. Diagnósticos, aptitud, sanciones o atribución de responsabilidad requieren garantías profesionales y jurídicas. En situaciones críticas puede automatizarse una parada protectora previamente diseñada, pero su lógica debe someterse a análisis de peligros. La pregunta adecuada no es si la IA reemplaza al especialista, sino qué combinación de automatización y juicio reduce el riesgo sin degradar derechos ni capacidad colectiva.

2.5. Visualizar para comprender y actuar

La visualización convierte datos en una representación que facilita comparar, localizar y reconocer cambios. Un tablero de SST no es una colección decorativa de gráficos; es una interfaz de decisión. Debe responder a preguntas concretas: qué condición requiere atención, dónde se concentra, cómo evoluciona y qué acción está pendiente. La selección de indicadores comienza por el usuario y su horizonte: la sala de control necesita segundos, la supervisión diaria necesita tareas y la dirección requiere tendencias y efectividad de controles.

Los indicadores rezagados —lesiones, días perdidos, enfermedades reconocidas— describen consecuencias. Los adelantados observan condiciones y capacidad: funcionamiento de barreras, exposición, cierre de acciones, mantenimiento o calidad de inspecciones. Un tablero equilibrado evita sustituir prevención por conteo de actividades. Cerrar muchas observaciones no

demuestra reducción de riesgo si las acciones son superficiales; a su vez, una baja tasa de incidentes puede coexistir con barreras degradadas.

La forma gráfica debe corresponder a la relación. Las líneas muestran evolución; los mapas, distribución espacial; los diagramas de control, variación frente a una línea base; y las matrices permiten comparar áreas y riesgos. Los gráficos tridimensionales, escalas truncadas y exceso de color dificultan interpretación. El color no debe ser el único canal, porque parte de la población no distingue ciertas combinaciones. Etiquetas, unidades, periodo y fuente deben estar visibles.

La jerarquía visual orienta la atención sin esconder incertidumbre. Un indicador crítico puede situarse primero, seguido de tendencia, contexto y acciones. La posibilidad de profundizar desde un resumen hasta registros permite investigar sin saturar la pantalla. El acceso a datos personales debe restringirse; muchos tableros pueden operar con agregación. Las celdas pequeñas o grupos reducidos pueden permitir reidentificación, por lo que requieren supresión o combinación.

Cada indicador necesita ficha técnica: definición, numerador, denominador, periodicidad, fuente, responsable y limitaciones. Los cambios metodológicos deben marcarse en la serie para no confundirlos con mejora. Un tablero también necesita fecha de actualización y estado de calidad. Si faltan datos de una planta, el total no debería mostrarse como completo.

La validación se realiza con usuarios. Las pruebas deben observar si una persona identifica correctamente prioridad, tendencia y acción bajo tiempo limitado. Los errores de interpretación son fallas de diseño, no necesariamente falta de capacitación. Después del despliegue conviene analizar qué vistas se usan, qué alertas se atienden y si las decisiones mejoran. La visualización cumple su función cuando reduce la distancia entre evidencia y control efectivo.

2.6. Simular situaciones críticas sin poner vidas en peligro

La simulación representa sistemas, tareas o emergencias para explorar su comportamiento sin reproducir el peligro real. Puede adoptar ejercicios de escritorio, modelos matemáticos, entornos de RV o gemelos digitales

conectados con datos. Su ventaja es ensayar eventos infrecuentes, variar condiciones y repetir decisiones; su límite es la fidelidad. Toda simulación simplifica, y una representación convincente puede ocultar supuestos incorrectos.

El diseño comienza con objetivos verificables. Si se busca entrenar evacuación, deben definirse conductas, señales y criterios de desempeño; si se analiza un proceso, se especifican variables, relaciones y escenarios. La fidelidad relevante no siempre es visual. Para aprender una secuencia, la interacción y la retroalimentación pueden importar más que el realismo gráfico. Para evaluar tiempos de escape, la geometría, densidad y comportamiento requieren validación.

Los escenarios deben incluir variabilidad. Un ejercicio repetido con la misma ruta enseña a memorizar, no a decidir. Cambiar humo, bloqueo, comunicaciones o disponibilidad de equipos permite evaluar adaptación. Sin embargo, introducir demasiados eventos a la vez impide atribuir errores. La complejidad debe crecer con la competencia y acompañarse de una sesión posterior donde se revisen decisiones, emociones, fallas del sistema y medidas de mejora.

La simulación no reemplaza prácticas físicas indispensables ni certificaciones. Puede preparar para ellas, reducir exposición inicial y permitir repetición. Tampoco debe utilizarse para probar tolerancia individual a condiciones extremas. El propósito es mejorar diseño, coordinación y respuesta. Los hallazgos deben integrarse al sistema de gestión mediante acciones, responsables y nueva verificación.

2.6.1. Realidad virtual y aprendizaje inmersivo

La RV sitúa al usuario en un entorno digital interactivo mediante visores y controladores. En seguridad puede representar alturas, incendios, espacios confinados, tránsito interno o procedimientos de bloqueo sin introducir el peligro físico. La revisión y metaanálisis de Scorgie et al. (2024) encontró efectos favorables de la RV en resultados de capacitación, aunque la magnitud depende del diseño, el comparador y la medida. Stefan et al. (2023) también señalan heterogeneidad y necesidad de evaluaciones más consistentes.

El aprendizaje inmersivo resulta adecuado cuando la competencia exige reconocer señales espaciales, practicar secuencias o decidir bajo presión. La experiencia debe construirse alrededor de objetivos, no de efectos visuales. Instrucciones breves, práctica guiada, retroalimentación inmediata y repetición espaciada ayudan a consolidar desempeño. Las métricas pueden incluir errores, tiempo, trayectoria, cumplimiento de pasos y transferencia a una tarea real.

La transferencia es el criterio principal. Recordar un procedimiento dentro del visor no garantiza aplicarlo en la planta. Una evaluación robusta combina prueba inmediata, retención posterior y observación en un entorno controlado. También compara con alternativas: instrucción presencial, video, simulador físico o modalidad mixta. La RV se justifica cuando mejora aprendizaje, acceso o seguridad con un costo razonable.

El cibermareo, la fatiga visual y las limitaciones de movilidad requieren detección y opciones. Las sesiones deben ser graduadas, con espacio seguro, higiene del equipo y posibilidad de abandonar sin penalización. El diseño debe considerar personas que usan lentes, tienen discapacidad, embarazo o condiciones susceptibles. Ofrecer una modalidad equivalente evita convertir la innovación en barrera.

Los datos de interacción pueden revelar dónde una persona mira, cuánto tarda y qué errores comete; son valiosos y sensibles. Debe explicarse qué se registra y evitar usos disciplinarios no previstos. La retroalimentación conviene centrarse en conducta y sistema, no en humillar ni provocar miedo. Los escenarios traumáticos necesitan cuidado adicional y apoyo.

Una implementación gradual incluye prototipo, prueba técnica, revisión por especialistas, piloto con usuarios y evaluación de transferencia. Los escenarios se actualizan cuando cambia el proceso. Una sala inmersiva desactualizada puede enseñar rutas o controles incorrectos con gran poder persuasivo. Versionado y aprobación deben tratarse con el mismo rigor que un procedimiento.

2.6.2. Gemelos digitales y representación de escenarios

Un gemelo digital es una representación dinámica de un activo, proceso o sistema que intercambia datos con su contraparte física. Se diferencia de un modelo estático porque actualiza estados y puede apoyar monitoreo, simulación o predicción. Zio (2024) revisa su uso en análisis de seguridad, evaluación de riesgos y gestión de emergencias, y muestra un campo prometedor pero aún marcado por desafíos de validación, interoperabilidad e incertidumbre.

La arquitectura reúne el sistema físico, sensores, comunicaciones, modelo, datos históricos y una interfaz. El gemelo puede representar una máquina, una línea, un edificio o una operación. En mantenimiento, combina condición actual y modelos de degradación; en emergencias, simula rutas bajo cambios de humo o bloqueo; en ergonomía, explora configuraciones. No todos los casos requieren tiempo real. La frecuencia de sincronización debe corresponder a la decisión.

Construir un gemelo empieza delimitando alcance y fidelidad. Intentar reproducir cada detalle aumenta costo y dificulta validación. El modelo debe incluir variables que modifican el riesgo y documentar las que excluye. Las condiciones iniciales, parámetros y reglas necesitan trazabilidad. La incertidumbre de sensores y modelos debe propagarse hacia resultados; presentar una única trayectoria puede ocultar varios escenarios plausibles.

La validación compara salidas con observaciones y con casos conocidos. Para eventos raros pueden utilizarse pruebas de componentes, datos históricos, análisis de sensibilidad y juicio experto estructurado. La calibración no debería usar los mismos datos que luego se presentan como validación. Cuando el gemelo recomienda una acción crítica, se requiere conocer en qué dominio funciona y qué condiciones invalidan la recomendación.

El valor más inmediato suele estar en comparar escenarios: cambiar ventilación, rutas, dotación, secuencia o mantenimiento antes de intervenir la planta. El resultado no es una profecía, sino una estimación condicionada. Un escenario “más seguro” puede trasladar riesgo a otra zona o grupo, por lo que la evaluación debe abarcar el sistema y la jerarquía de controles. Las personas que ejecutan el trabajo ayudan a detectar supuestos irreales.

La ciberseguridad es parte de la seguridad física cuando el gemelo recibe o envía información operacional. Datos manipulados pueden producir diagnósticos erróneos; una interfaz de control mal protegida puede abrir una vía hacia equipos. Segmentación, autenticación, integridad, copias, monitoreo y respuesta a incidentes forman parte del diseño. Si el gemelo interviene sobre el proceso, deben existir límites, aprobación y estados seguros.

Una ruta de adopción razonable avanza desde un caso delimitado. La organización identifica una decisión de alto valor, construye un modelo mínimo, valida datos y compara el resultado con la práctica existente. El piloto incluye escenarios normales y extremos, participación de usuarios y criterios de parada. Solo después se conecta a fuentes adicionales o a funciones automáticas. Esta progresión hace visibles los costos y evita que un proyecto de infraestructura pierda la pregunta preventiva que lo originó.

La evaluación combina desempeño técnico, utilidad operacional y efecto humano. En el plano técnico se revisan error, latencia, disponibilidad y robustez; en el operacional, calidad de decisiones, tiempo de respuesta y efectividad de controles; en el humano, comprensión, carga, confianza y equidad. Un gemelo puede reproducir con precisión una máquina y fracasar si nadie entiende su interfaz. También puede ser aceptado y, aun así, no modificar la exposición. Las tres dimensiones deben sostenerse simultáneamente.

La convergencia de sensores, Big Data, IA, visualización y simulación ofrece una capacidad preventiva que antes era difícil alcanzar: observar cambios, reconocer combinaciones, ensayar controles y aprender de la respuesta. Esa capacidad solo se materializa cuando la cadena completa es confiable. La calidad del dato, la participación, la supervisión humana y la acción sobre las causas mantienen la tecnología dentro de su función: apoyar una prevención más temprana, comprensible y verificable.

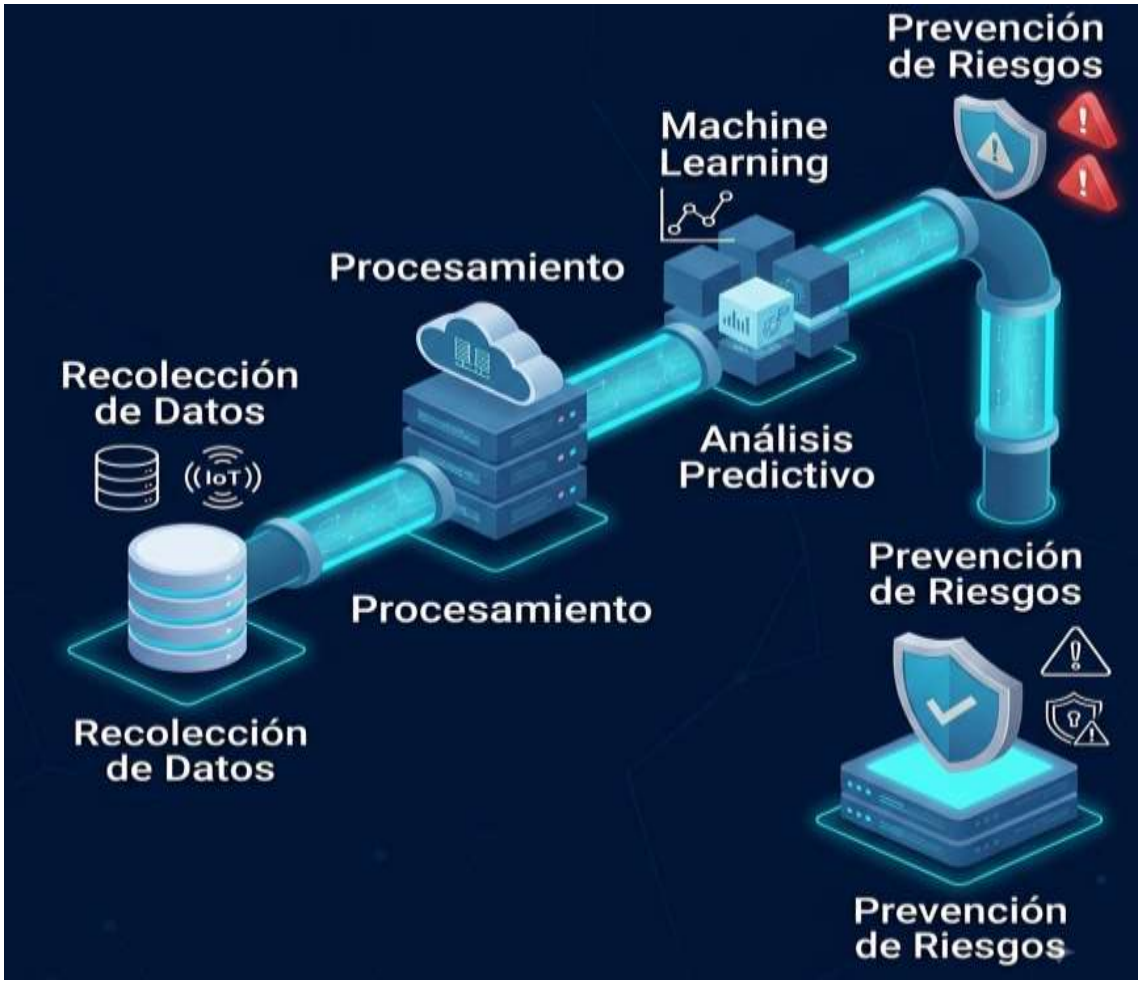
La secuencia práctica puede resumirse como un ciclo de aprendizaje: formular una decisión, medir lo necesario, comprobar la calidad, interpretar con el trabajo real, actuar y evaluar el resultado. Si una fase falla, la sofisticación de las demás no la compensa. La captura sin gobernanza crea vigilancia; la predicción sin intervención produce expectativas; la visualización sin responsable se convierte

en contemplación, y la automatización sin supervisión desplaza riesgos. Cuando el ciclo se diseña desde la prevención, la tecnología ayuda a hacer visibles señales débiles y a intervenir con mayor oportunidad, sin confundir la recomendación digital con el juicio definitivo sobre las personas o el sistema.

La madurez, por tanto, no se mide por el número de dispositivos instalados. Se reconoce en la capacidad de detectar una desviación, explicar sus límites, responder a tiempo y demostrar que el control aplicado redujo la exposición sin trasladar el daño.

Figura 2.

Analítica de Datos y Modelos Predictivos



Capítulo III: Llevar la innovación al lugar donde ocurre el trabajo

Llevar la innovación al lugar donde ocurre el trabajo

Una tecnología preventiva adquiere valor cuando modifica una condición de trabajo antes de que produzca daño. La afirmación parece evidente, pero numerosos proyectos se concentran en instalar equipos, activar licencias o mostrar indicadores y dejan para después la organización de la respuesta. El resultado puede ser un sistema que detecta desviaciones con precisión y, aun así, no reduce la exposición porque nadie sabe quién debe actuar, el aviso llega fuera de contexto o las personas evitan utilizarlo. Llevar la innovación al lugar de trabajo significa cerrar esa distancia entre capacidad técnica y acción cotidiana.

La implementación ocurre dentro de relaciones, rutinas, restricciones y saberes previos. Una alarma digital entra en un turno con prioridades productivas; un dispositivo portátil se coloca sobre un cuerpo que ya usa equipos de protección; una aplicación compite con formularios y canales existentes; una plataforma de teletrabajo modifica ritmos, disponibilidad y supervisión. La tecnología nunca se añade a un espacio vacío. Cambia tareas, distribuye información y puede trasladar responsabilidades, incluso cuando el proyecto se presenta como una mejora exclusivamente técnica.

La evidencia reciente propone un enfoque centrado en las personas. La revisión de Mendes et al. (2026) sobre tecnologías portátiles en seguridad y salud en el trabajo (SST) identifica barreras técnicas, organizacionales, éticas y humanas, junto con evidencia todavía limitada sobre efectos sostenidos. La Organización Internacional del Trabajo (OIT, 2025) reconoce que la digitalización puede reducir exposiciones y apoyar la prevención, pero también introduce riesgos asociados con vigilancia, gestión algorítmica y nuevas modalidades laborales. Ambas perspectivas conducen a una misma exigencia: evaluar la solución por su integración con el sistema preventivo y no por su novedad.

Este capítulo desarrolla esa integración desde cuatro preguntas. La primera es si la organización comprende la necesidad y tiene madurez para sostener la solución. La segunda examina quién participa en el diseño y si el resultado es usable, accesible e inclusivo. La tercera aborda la transformación de alertas en decisiones coordinadas. La cuarta contrasta aprendizajes de industria, construcción, salud, servicios, teletrabajo y territorios complejos. El hilo común

es la adaptación recíproca, con un límite claro: el trabajo puede reorganizarse para aprovechar una herramienta, pero nunca a costa de crear riesgos o exigir que las personas compensen sus defectos.

3.1. Antes de incorporar tecnología: escuchar y comprender

La fase previa no comienza con una demostración comercial, sino con una descripción compartida del problema. ¿Qué daño se quiere evitar? ¿En qué tareas aparece? ¿Qué controles existen y por qué no son suficientes? ¿Qué decisión podría mejorar con información adicional? Estas preguntas impiden que la organización confunda una solución disponible con una necesidad real. También permiten reconocer si el problema requiere tecnología o una intervención más directa, como sustituir un material, reparar ventilación, cambiar una secuencia o aumentar dotación.

Escuchar implica observar el trabajo tal como se ejecuta. Los procedimientos muestran la tarea prescrita; recorridos, entrevistas y conversaciones de turno revelan ajustes, interrupciones y presiones. Quien realiza la actividad conoce señales débiles que no aparecen en estadísticas: un ruido antes de una falla, una zona sin cobertura, una alarma que se activa durante una maniobra normal o un guante que impide manipular una pantalla. Ese conocimiento no sustituye mediciones, pero ayuda a decidir qué medir y cómo interpretar el resultado.

La indagación debe incluir diversidad de roles y condiciones. Supervisores, mantenimiento, contratistas, personal nocturno, trabajadores temporales, mujeres, personas mayores, jóvenes y quienes presentan discapacidad pueden experimentar una misma herramienta de maneras distintas. Si se consulta solo a usuarios expertos del turno diurno, la solución reflejará ese segmento. La Agencia Europea para la Seguridad y la Salud en el Trabajo destaca que comunicación, formación y participación directa son elementos centrales para implementar sistemas digitales inclusivos (European Agency for Safety and Health at Work [EU-OSHA], 2023a).

Conviene separar síntoma, causa y oportunidad. La tardanza en reportar un peligro puede deberse a un formulario largo, pero también a temor a represalias, ausencia de respuesta previa o falta de tiempo. Digitalizar el formulario resolvería una fricción y conservaría las demás. Un mapa de actores, tareas, decisiones y

barreras permite reconocer dónde se pierde información y dónde se detiene la acción. La solución se define después de ese diagnóstico.

La escucha también establece criterios de éxito. “Mejorar la seguridad” es demasiado amplio; resultan evaluables objetivos como reducir el tiempo entre detección y aislamiento, aumentar la cobertura de una exposición, disminuir errores en un procedimiento o mejorar la calidad del cierre de acciones. Los criterios deben incluir efectos no deseados: carga adicional, falsas alarmas, exclusión, invasión de privacidad o transferencia de riesgo. De esta manera, el piloto puede detenerse o modificarse antes de escalar.

3.1.1. Reconocer necesidades, temores y expectativas

Las necesidades se expresan en distintos niveles. Una persona puede pedir una alarma más visible; el equipo puede necesitar un canal de escalamiento; la organización quizá requiera rediseñar la barrera que genera avisos frecuentes. Registrar la petición literal es solo el inicio. Técnicas como entrevistas semiestructuradas, observación contextual, talleres y reconstrucción de incidentes ayudan a identificar la función buscada. La pregunta no es qué dispositivo desea el usuario, sino qué dificultad intenta resolver.

Los temores aportan información de diseño. La preocupación por vigilancia puede indicar que no están claros la finalidad, el acceso o las consecuencias de los datos. El miedo a ser reemplazado revela incertidumbre sobre cambios de tareas. La resistencia a una alarma puede provenir de experiencias con falsos positivos. Tratar estas respuestas como ignorancia bloquea el diálogo; examinarlas permite ajustar gobernanza, interfaz, formación y límites de uso.

La privacidad merece acuerdos concretos. Debe explicarse qué se recoge, con qué frecuencia, si se identifica a la persona, dónde se conserva y quién puede consultarlo. También qué no se hará: por ejemplo, no emplear datos fisiológicos para sancionar rendimiento ni trayectorias de proximidad para controlar pausas. Las promesas deben incorporarse a políticas, permisos y contratos, porque una explicación verbal no protege frente a usos futuros. Cuando sea posible, el procesamiento local y la agregación reducen exposición de datos.

Las expectativas pueden ser excesivas en ambos sentidos. La dirección puede esperar que la inteligencia artificial (IA) prediga todo accidente; los trabajadores, que la alarma elimine el peligro; el proveedor, que el uso crezca sin cambios de proceso. La conversación temprana delimita capacidades e incertidumbre. Un sistema de visión puede reconocer una condición definida, pero no comprender toda la tarea; un wearable puede señalar una postura, pero no decidir por sí solo el rediseño ergonómico.

La confianza se construye con evidencia y capacidad de cuestionamiento. Un piloto transparente muestra errores y decisiones de corrección. También ofrece un canal para reportar fallas sin penalización. Si la organización oculta limitaciones para proteger el entusiasmo del proyecto, cada error posterior deteriora credibilidad. La aceptación no equivale a obediencia: una persona puede comprender la finalidad y aun rechazar una solución que interfiere con su seguridad o dignidad.

La devolución cierra la escucha. Quienes participaron necesitan conocer qué se aprendió, qué propuestas se aceptaron, cuáles no y por qué. Sin retorno, la consulta se percibe como una ceremonia. La trazabilidad de aportes ayuda a distribuir poder y evita que solo las voces con mayor jerarquía definan el diseño. Baines et al. (2022), en una revisión amplia sobre participación en innovación digital en salud, encontraron que las personas suelen incorporarse tarde, cuando apenas pueden influir; aunque el campo sea diferente, la lección de involucramiento temprano es directamente pertinente para la SST.

Las entrevistas deben proteger la calidad del relato. Preguntar frente a la jefatura si una herramienta inspira confianza suele producir respuestas prudentes; conversar en espacios separados y garantizar que los comentarios se presentarán de forma agregada amplía la información. También conviene incluir a quienes abandonaron una prueba, porque sus razones pueden revelar barreras que los usuarios persistentes ya aprendieron a tolerar. La saturación no se alcanza por número fijo: se revisa si aparecen perspectivas nuevas entre grupos y turnos.

Las expectativas se ordenan con escenarios de uso y de no uso. El primero describe cuándo se activa, quién recibe y qué decisión apoya; el segundo

delimita situaciones para las cuales no fue validada. Este contraste evita que una aplicación concebida para observación ergonómica termine utilizada como diagnóstico o control disciplinario. Los límites deben aparecer en la interfaz y la formación, no únicamente en documentación legal que casi nadie consulta.

3.1.2. Evaluar la madurez digital de la organización

La madurez digital no es un inventario de computadores. Describe la capacidad de gobernar datos, integrar sistemas, desarrollar competencias, gestionar cambios y convertir resultados en decisiones. Una organización puede contar con sensores avanzados y mantener registros incompatibles, responsabilidades difusas o respuestas manuales sin seguimiento. En esas condiciones, añadir tecnología aumenta complejidad antes que prevención.

Los modelos de madurez suelen evaluar estrategia, procesos, tecnología, datos, personas y cultura. Cognet et al. (2023), al comparar sistemáticamente modelos de evaluación, muestran gran diversidad de dimensiones y escalas; por ello, no existe una calificación universal que deba aplicarse sin adaptación. Para SST conviene añadir gobernanza ética, participación, ciberseguridad, capacidad de respuesta y alineación con la jerarquía de controles.

La evaluación puede organizarse en cinco preguntas. Primero, si el problema y el propósito están definidos. Segundo, si los datos son suficientes, confiables e interoperables. Tercero, si existe infraestructura con mantenimiento y soporte. Cuarto, si las personas tienen tiempo, competencia y autoridad. Quinto, si la organización puede aprender del piloto y retirar la solución cuando no aporta valor. Cada respuesta necesita evidencia: procedimientos, registros, pruebas, entrevistas y observación.

La preparación de datos incluye diccionarios, responsables, reglas de calidad y acceso. La preparación técnica abarca cobertura, energía, compatibilidad, actualizaciones y modos seguros ante fallas. La organizacional exige presupuesto de ciclo de vida, no solo compra inicial. La humana considera alfabetización digital, carga, participación y confianza. Una debilidad crítica puede justificar un piloto limitado o trabajo preparatorio antes de implementar.

La madurez no debe convertirse en una barrera que excluya pequeñas empresas. Un enfoque gradual permite comenzar con procesos simples y controlados: digitalizar una inspección bien definida, mejorar el cierre de acciones o instalar un sensor en una condición prioritaria. El objetivo no es alcanzar el nivel más alto de una escala, sino sostener la solución apropiada. Una hoja de cálculo gobernada puede ser más madura que una plataforma compleja sin propietarios ni validación.

El diagnóstico debe reconocer dependencias externas. Proveedores, conectividad, servicios en la nube y repuestos pueden determinar continuidad. En América Latina, diferencias de infraestructura y competencias entre sedes exigen planes por contexto. La obra *Salud digital 4.0* examina interoperabilidad, trazabilidad, privacidad y brechas regionales en sistemas sanitarios, problemas transferibles con cautela a la gestión ocupacional (Rodríguez-Lindao et al., 2026). Copiar una arquitectura diseñada para una gran institución puede dejar sin soporte a operaciones pequeñas o remotas.

Una matriz de preparación ayuda a decidir entre avanzar, acondicionar o detener. Los criterios de “no avanzar” son tan importantes como los de aprobación: ausencia de finalidad legítima, riesgo alto de vigilancia, incapacidad para responder a alertas, incompatibilidad con equipos de protección o falta de validación en la población. Posponer no significa rechazar innovación; puede ser la decisión preventiva más responsable.

La madurez puede evaluarse mediante niveles descriptivos, evitando un puntaje que oculte diferencias. Una organización podría tener alta infraestructura y baja gobernanza, o equipos competentes con conectividad insuficiente. El perfil por dimensiones orienta inversiones: mejorar el catálogo de datos, formar supervisores, establecer soporte o fortalecer comités. Repetir la evaluación después del piloto permite observar aprendizaje sin convertirla en examen punitivo.

También se necesita una línea base. Antes de instalar, se miden tiempos, errores, exposiciones, reportes y carga con métodos comparables. Sin ella, cualquier cambio favorable puede atribuirse a la tecnología aunque provenga de mayor atención durante el piloto. La línea base debe cubrir variabilidad suficiente

y registrar intervenciones concurrentes. Cuando no puede medirse un resultado final, se eligen indicadores intermedios ligados de manera razonable al control.

3.2. Diseñar soluciones con quienes viven el riesgo

El diseño participativo reconoce a los trabajadores como productores de conocimiento y no solo como usuarios finales. Ellos conocen variaciones, atajos, señales y restricciones que un equipo externo observa durante poco tiempo. Integrar ese saber modifica requisitos, prioridades y criterios de prueba. También hace visibles consecuencias distributivas: quién recibe beneficios, quién asume carga y quién queda sometido a mayor observación.

Participar no significa elegir el color de una pantalla una vez construida. La influencia debe comenzar en la definición del problema y continuar en prototipos, pruebas, despliegue y revisión. Cada etapa admite técnicas distintas: recorridos y mapas de experiencia para comprender; bocetos y simulaciones para explorar; pruebas en contexto para validar; y reuniones de revisión para aprender. Las personas necesitan tiempo laboral, información y posibilidad real de disentir.

La composición del grupo importa. Los participantes más disponibles o familiarizados con tecnología no representan toda la operación. Un muestreo intencional incluye turnos, ocupaciones, contratos, edades, idiomas y capacidades diversas. Cuando existen relaciones jerárquicas fuertes, conviene ofrecer espacios separados o mecanismos confidenciales. La presencia de un supervisor puede inhibir comentarios sobre presión productiva o uso disciplinario.

La participación debe conectarse con decisiones. Un registro puede vincular necesidad, propuesta, cambio, responsable y resultado. Algunas solicitudes serán incompatibles entre sí o con requisitos técnicos; explicar el criterio preserva legitimidad. El equipo de diseño conserva responsabilidades profesionales y legales, pero no monopoliza el problema. La coproducción no elimina conflictos: los hace discutibles antes de que aparezcan durante el uso.

3.2.1. Participación de los trabajadores en el diseño

La primera contribución es delimitar escenarios. Un mismo sensor puede funcionar en mantenimiento planificado y fallar en una emergencia. Los

trabajadores ayudan a describir variaciones de carga, clima, herramientas, prendas y comunicación. Los escenarios deben incluir condiciones normales, degradadas y excepcionales. Diseñar solo para el flujo ideal produce soluciones frágiles.

Los prototipos de baja fidelidad tarjetas, diagramas o pantallas impresas permiten discutir sin invertir en código. Un grupo puede ordenar alertas, cambiar palabras y señalar información ausente. Después, un prototipo funcional prueba interacción y tiempos. Esta progresión reduce el costo de modificar y evita que una interfaz pulida parezca inamovible. La pregunta de cada sesión debe ser precisa para no convertir la participación en una aprobación general.

Los pilotos necesitan acuerdos sobre voluntariedad, datos y soporte. Si participar puede afectar la evaluación laboral, la libertad es dudosa. Debe aclararse cómo reportar molestias, detener el uso y recibir atención si aparece un hallazgo fisiológico. El consentimiento no reemplaza la obligación de prevenir ni legitima condiciones inseguras. Tampoco debería descargarse sobre cada trabajador una decisión que corresponde a gobernanza colectiva.

La retroalimentación se observa además del relato. Una persona puede decir que una aplicación es sencilla y, aun así, tardar demasiado o omitir pasos. Las pruebas combinan desempeño, comprensión, carga percibida y conversación. Registrar video o pantalla requiere autorización y minimización de datos. Los errores se analizan como interacción entre persona, diseño y contexto, no como incompetencia individual.

El poder de decisión debe ser visible. Pueden definirse materias consultivas, compartidas y no negociables. Las exigencias legales no se someten a votación, pero la manera de cumplirlas sí puede diseñarse conjuntamente. Los trabajadores deberían tener capacidad para detener una prueba que introduce peligro y acceso a resultados agregados. La representación sindical o comités de SST aporta continuidad más allá del grupo piloto.

La revisión sistemática de Baines et al. (2022) identificó que tiempo, recursos, comunicación clara y distribución de poder condicionan la participación significativa. Su aplicación a la SST exige remunerar o reconocer el tiempo, facilitar idiomas y evitar que la consulta recaiga siempre en las mismas personas.

La participación de calidad puede alargar la fase inicial y acortar correcciones posteriores.

La representación sostenida necesita renovación. Si siempre participan los mismos trabajadores, pueden desarrollar lenguaje técnico y alejarse de experiencias recientes. Rotar integrantes, mantener representantes experimentados e incorporar nuevas voces equilibra continuidad y diversidad. Los materiales preparatorios deben ser comprensibles y compartirse con antelación; pedir una opinión inmediata sobre un sistema complejo favorece a quienes ya dominan la tecnología.

El codiseño también puede revelar que la mejor solución no es digital. Durante un taller, un equipo puede identificar que una barrera física, una etiqueta o un cambio de ruta resuelve el problema con menos dependencia. Esta conclusión no debe interpretarse como fracaso del proyecto. El criterio de éxito es controlar el riesgo, y la tecnología solo conserva preferencia cuando aporta una ventaja demostrable frente a opciones más simples.

3.2.2. Usabilidad, accesibilidad e inclusión

La usabilidad relaciona efectividad, eficiencia y satisfacción con usuarios, tareas y contextos concretos. No es una propiedad fija de la interfaz. Una pantalla legible en oficina puede fallar bajo sol, lluvia, ruido, guantes o presión temporal. La prueba debe reproducir condiciones relevantes sin exponer a peligro. Tiempo, errores, recuperación y comprensión ofrecen evidencia más útil que preguntar si “gustó” el sistema.

La accesibilidad busca que personas con capacidades diversas perciban, comprendan y operen la solución. Incluye contraste, tamaño, lenguaje claro, alternativas al color, señales visuales y hápticas, subtítulos y compatibilidad con tecnologías de apoyo. En entornos ruidosos, una alarma solo sonora excluye y puede pasar inadvertida; una vibración única puede confundirse con otra notificación. La redundancia multimodal debe distinguir prioridades sin saturar.

La inclusión amplía la mirada hacia edad, idioma, alfabetización, género, cultura y situación contractual. Un wearable diseñado sobre medidas corporales limitadas puede ajustar mal; el reconocimiento de imágenes puede rendir de

forma desigual con tonos de piel, prendas o equipos; una aplicación textual puede excluir a quienes dominan otro idioma. EU-OSHA (2023a) señala que los sistemas digitales pueden apoyar a trabajadores mayores, migrantes, jóvenes, embarazadas o neurodiversos si sus necesidades se incorporan desde el diseño.

El lenguaje de las alertas debe ser directo y accionable. “Anomalía 47” no ayuda bajo presión. El mensaje necesita indicar condición, ubicación, gravedad, conducta inmediata y vía de confirmación. Los iconos se prueban, porque su significado no es universal. La traducción debe revisar términos técnicos y comprensión, no limitarse a equivalencias literales.

La carga cognitiva aumenta cuando proliferan aplicaciones, contraseñas y notificaciones. Integrar canales y reducir entradas evita que el trabajador gestione la complejidad del sistema. Las tareas críticas deben requerir pocos pasos y ofrecer confirmación. El diseño tolerante a errores permite corregir sin perder información y evita acciones irreversibles accidentales. En una emergencia, la autenticación puede necesitar un mecanismo seguro que no retrase la respuesta.

La accesibilidad incluye la posibilidad de no usar un dispositivo cuando existen razones justificadas. Una alternativa equivalente protege a personas con condiciones médicas, discapacidad o incompatibilidad con equipos. La solución no debería convertir una característica personal en motivo de exclusión laboral. Las evaluaciones deben documentar quiénes participaron y qué grupos faltan, evitando afirmar universalidad con muestras estrechas.

Las pruebas incorporan situaciones de estrés sin inducir peligro. Un usuario puede comprender una pantalla durante una sesión tranquila y equivocarse cuando lleva protección respiratoria o atiende varias señales. La evaluación gradúa carga, ruido e interrupciones dentro de un entorno controlado. Se observa no solo si completa la tarea, sino si reconoce el error y se recupera. Los resultados orientan simplificación y redundancia.

La inclusión requiere revisar resultados después del despliegue. Tasas de falsas alarmas, abandono, tiempo y solicitudes de ayuda se comparan entre grupos cuando es legítimo y seguro hacerlo. Una diferencia no debe usarse para etiquetar a las personas; activa una investigación del ajuste, la formación y el

algoritmo. Las categorías demográficas se recogen únicamente con finalidad definida y protección adecuada.

3.2.3. Adaptar la tecnología al contexto, no el contexto a la tecnología

Adaptar al contexto significa respetar la tarea, el ambiente, la infraestructura y el sistema de control. No implica congelar prácticas: algunos procesos deben cambiar para mejorar seguridad. El criterio consiste en distinguir entre rediseñar el trabajo para eliminar un peligro y forzar a las personas a compensar limitaciones de una herramienta. Si un sensor solo funciona sin guantes, la respuesta no es retirar protección.

La configuración comienza con parámetros locales. Umbrales, zonas, frecuencias y destinatarios pueden variar por proceso. Utilizar valores predeterminados sin validación genera alarmas irrelevantes o silencios peligrosos. Cada ajuste necesita responsable, versión y prueba. La personalización excesiva también puede fragmentar; por eso se conserva un núcleo común y se documentan excepciones.

La infraestructura define modos de operación. En lugares con conectividad intermitente, el dispositivo debe conservar funciones críticas sin nube, almacenar datos y sincronizar cuando regrese la red. La batería debe cubrir el turno con margen; los cargadores, repuestos y calibración requieren logística. En climas extremos se prueban temperatura, humedad, polvo y resistencia. La robustez no puede inferirse de una ficha comercial.

La integración con procedimientos evita dobles sistemas. Si una alerta digital y un formulario en papel siguen rutas distintas, nadie sabe cuál prevalece. Mapear entradas, decisiones y cierres ayuda a eliminar duplicidad. Durante la transición puede mantenerse redundancia, pero con plazo y reglas claras. La interoperabilidad también reduce transcripción y errores, siempre que no propague datos defectuosos.

El ajuste organizacional incluye turnos, contratistas y mantenimiento. Una plataforma que solo reconoce empleados directos deja huecos en operaciones mixtas. Los contratos deben definir formación, acceso y respuesta sin trasladar

obligaciones. El soporte fuera del horario diurno resulta esencial si la operación es continua. Una alarma nocturna sin especialista disponible crea una falsa capacidad.

Dodoo et al. (2024), en su revisión de innovaciones digitales en industrias peligrosas, identifican beneficios junto con problemas de alineación, costo, privacidad y resistencia. La lección no es evitar herramientas, sino evaluar su encaje técnico, conductual y organizacional. La adaptación termina cuando el uso se estabiliza y comienza de nuevo ante cambios de personal, proceso, software o riesgo.

La gestión de configuración evita que cada sede cree una versión irreconocible. Los parámetros locales se guardan en un registro común con motivo, aprobador y fecha. Las actualizaciones se ensayan en un entorno controlado y se despliegan gradualmente. Si se detecta una falla, la organización puede identificar versiones afectadas y volver a un estado conocido. Este control resulta especialmente importante cuando una plataforma modifica reglas desde la nube.

La dependencia de proveedor se reduce exigiendo formatos exportables, documentación y acuerdos de continuidad. Una organización debe poder recuperar su historial y mantener controles esenciales si termina el contrato. El costo de migración forma parte de la evaluación inicial. Las soluciones cerradas pueden ser apropiadas, pero su conveniencia debe compararse con la pérdida de autonomía y la disponibilidad de soporte regional.

3.3. De la alerta a la acción preventiva

Una alerta es una comunicación sobre una condición que requiere atención. Su valor depende de oportunidad, comprensión y capacidad de respuesta. Los sistemas suelen evaluarse por sensibilidad o velocidad, mientras la cadena humana queda implícita. Para prevenir, el aviso debe llegar a quien puede decidir, con autoridad, recursos y tiempo.

La cadena puede representarse como detección, validación, clasificación, comunicación, acción y cierre. Cada eslabón tiene fallas: sensor sin calibrar, regla errónea, mensaje ambiguo, destinatario ausente, acción no autorizada o cierre sin verificación. El diseño debe probar el recorrido completo. Una

demostración que termina cuando aparece una notificación no valida el sistema preventivo.

Las alertas necesitan niveles de criticidad asociados con conductas. Un evento informativo alimenta tendencias; una advertencia exige revisión; una alarma crítica puede activar evacuación o parada. Las definiciones deben basarse en gravedad, probabilidad, velocidad de evolución y reversibilidad. Colores y sonidos ayudan, pero la clasificación debe quedar expresada en palabras y procedimientos.

La fatiga aparece cuando el volumen supera la capacidad o las señales carecen de acción. Silenciar individualmente puede ocultar peligros. La mejora consiste en analizar duplicados, umbrales, agrupación y causas recurrentes. Si una condición genera alarmas diarias, quizá el problema es el proceso, no el sistema. El indicador útil no es cuántas alertas se emitieron, sino cuántas condujeron a controles adecuados y qué exposiciones cambiaron.

El registro de alerta debe conservar la secuencia sin convertirse en un repositorio de datos innecesarios. Hora de detección, recepción, decisión, acción y verificación permiten localizar demoras. Las conversaciones o imágenes solo se almacenan si aportan evidencia y con acceso limitado. La retención se define por finalidad, obligaciones y valor de aprendizaje. Acumular todo “por si acaso” aumenta riesgo de privacidad y dificulta encontrar lo relevante.

Una revisión periódica compara desempeño con los supuestos originales. Puede ocurrir que el peligro cambie, que una barrera reduzca la frecuencia o que el equipo aprenda a responder de otra manera. En tal caso se ajustan umbrales, destinatarios o incluso se retira la alerta. Las reglas que nadie posee tienden a permanecer por inercia y llenan el sistema de señales antiguas.

3.3.1. ¿Quién decide cuando un sistema detecta un peligro?

La respuesta depende del tipo de decisión. Una parada automática previamente diseñada puede ser apropiada ante proximidad a maquinaria; una recomendación sobre fatiga requiere interpretación; una modificación de aptitud exige evaluación profesional y garantías. Clasificar las decisiones por impacto,

urgencia y reversibilidad permite asignar niveles de autonomía. No toda señal debe terminar en una persona, ni toda decisión puede delegarse al algoritmo.

El responsable primario debe estar nombrado por rol, con suplencia y escalamiento. “Notificar al área” es insuficiente. El procedimiento define quién recibe, cuánto tiempo tiene, qué puede ordenar y a quién informa. Si la acción requiere detener producción, la autoridad debe existir antes de la alarma. De lo contrario, el trabajador queda entre la advertencia y una presión incompatible.

La supervisión humana necesita información para cuestionar. Debe mostrar fuente, hora, ubicación, nivel de confianza, variables relevantes y limitaciones. Un puntaje sin explicación fomenta sesgo de automatización. El marco de gestión de riesgos de IA del National Institute of Standards and Technology propone gobernar, mapear, medir y gestionar durante el ciclo de vida (Tabassi, 2023). Aplicado a alertas, exige propietario, documentación, métricas, monitoreo y mecanismos de corrección.

La posibilidad de anular una recomendación debe diseñarse. En algunos casos el operador confirma una parada; en otros, puede restablecer después de verificar. Cada anulación registra motivo sin convertir al trabajador en sospechoso. Analizar discrepancias ayuda a detectar fallas del modelo, cambios del proceso o necesidad de formación. Una tasa alta de anulaciones no demuestra indisciplina.

Los proveedores no asumen la responsabilidad preventiva de la organización. Aunque administren la plataforma, el empleador y los profesionales competentes deben conocer límites y asegurar controles. Los contratos han de cubrir cambios de modelo, disponibilidad, incidentes, auditoría, portabilidad y eliminación de datos. Una actualización que modifica el comportamiento de alertas requiere evaluación antes de producción.

Las decisiones que afectan derechos necesitan mayor protección. Los datos de SST no deberían alimentar sanciones, despidos o selección sin fundamento legal, transparencia y revisión. Una inferencia de riesgo no prueba conducta culpable. Separar la función preventiva de la disciplinaria favorece reporte y confianza. La participación de comités de SST y protección de datos ayuda a establecer límites.

La rendición de cuentas se distribuye sin diluirse. El área técnica responde por infraestructura y cambios; el propietario del proceso, por la decisión; SST, por criterios preventivos; protección de datos, por tratamiento; y la dirección, por recursos y prioridades. Una matriz de responsabilidades puede aclarar quién ejecuta, aprueba, consulta e informa. Si todos son responsables en términos generales, nadie lo es ante un evento concreto.

En sistemas de alto impacto, un comité revisa incidentes, desempeño y cambios, pero no reemplaza la decisión urgente. La gobernanza opera antes y después: define límites y aprende. Durante la emergencia actúan roles entrenados. Separar ambos tiempos evita que una alarma crítica quede esperando una reunión o que una respuesta rápida modifique silenciosamente reglas permanentes.

3.3.2. Respuesta oportuna y coordinación de los equipos

La oportunidad se define por la dinámica del peligro. Segundos importan ante una colisión; horas pueden ser suficientes para una tendencia térmica; semanas pueden orientar un rediseño ergonómico. Medir un tiempo promedio mezcla situaciones distintas. Cada clase necesita objetivo, desde detección hasta control efectivo, y no solo hasta lectura del mensaje.

La coordinación exige un lenguaje común entre operación, SST, mantenimiento, salud ocupacional y emergencias. Una alerta de gas puede implicar aislamiento, verificación, evacuación y atención. Las responsabilidades se practican mediante ejercicios. Los directorios, canales y suplencias deben mantenerse actualizados; una cadena perfecta en el documento falla si depende de un teléfono sin cobertura.

El contexto que acompaña al aviso reduce llamadas y demoras. Ubicación, activo, tendencia, personas potencialmente expuestas y controles disponibles permiten decidir. Mostrar demasiados datos produce el efecto contrario. La interfaz debe ofrecer una vista breve y profundización. Durante eventos críticos conviene congelar información relevante para investigar después sin alterar la pantalla operacional.

El cierre requiere comprobar la condición y la eficacia. Marcar “atendido” no demuestra control. El responsable documenta acción provisional, acción definitiva y verificación. Si la alerta se originó por error, se registra causa técnica. Los eventos repetidos se agrupan para evitar cierres aislados. El aprendizaje llega a quienes diseñan reglas y a quienes ejecutan la tarea.

Los simulacros de extremo a extremo revelan latencia, ambigüedad y conflictos. Deben incluir pérdida de red, ausencia del responsable y alarmas simultáneas. No se trata de sorprender a las personas, sino de probar el sistema. Los resultados se convierten en acciones con plazo. Una plataforma crítica se revalida tras actualizaciones, cambios de proceso o incidentes.

La coordinación también considera carga emocional. Una alerta biométrica o de posible exposición puede causar ansiedad. El mensaje debe evitar diagnósticos y ofrecer una ruta de apoyo. En servicios de salud, donde el personal ya enfrenta interrupciones, las notificaciones adicionales pueden aumentar carga. La tecnología debe integrarse al flujo clínico u operacional y retirar señales de bajo valor.

Los indicadores de coordinación pueden incluir tiempo hasta reconocimiento, tiempo hasta control, porcentaje con responsable, reaparición y calidad de verificación. Medir solo rapidez puede incentivar cierres prematuros. Las métricas se interpretan con gravedad y complejidad, y se revisan con los equipos. Un caso lento porque exigió aislamiento complejo no es equivalente a una demora por destinatario ausente.

El relevo de turno es un punto vulnerable. Las alertas abiertas deben transferirse con estado, acciones provisionales y próximos pasos. La plataforma puede apoyar, pero la conversación sigue siendo necesaria en eventos críticos. Si el relevo se limita a una lista larga, las prioridades se pierden. Una vista específica de pendientes y riesgos residuales facilita continuidad.

3.4. Aprendizajes desde distintos escenarios laborales

La transferencia de una solución entre sectores requiere distinguir principios y configuraciones. Participación, gobernanza, validación y respuesta son principios generales; umbrales, interfaces, conectividad y procedimientos son

contextuales. Un caso exitoso ofrece preguntas y mecanismos, no una receta. La evidencia de laboratorio tampoco equivale a funcionamiento durante turnos, clima y presión reales.

Comparar escenarios permite reconocer patrones. En industrias de alto riesgo predominan sensores, automatización y barreras físicas; en servicios, información, carga cognitiva y privacidad; en teletrabajo, límites temporales y ergonomía distribuida; en territorios complejos, conectividad, mantenimiento y autonomía local. Las categorías se superponen: un hospital tiene riesgos industriales, una mina utiliza servicios digitales y una persona rural puede teletrabajar.

La evaluación debe incluir resultados técnicos, operacionales y humanos. Precisión y disponibilidad no bastan si no cambia la acción; satisfacción no basta si el riesgo permanece; reducción de incidentes puede ser inconcluyente cuando los eventos son raros. Una combinación de funcionamiento de barreras, exposición, tiempos, errores, aceptación y resultados de salud permite interpretar mejor.

Los casos deben documentar contexto y condiciones de implementación. “La empresa redujo incidentes” dice poco sin población, periodo, cambios concurrentes y definición. Una ficha transferible describe tarea, peligro, arquitectura, participación, gobernanza, costos, resultados y limitaciones. Los aprendizajes negativos son valiosos si explican por qué se detuvo o modificó el sistema. La transparencia reduce repetición de errores y contrapesa el sesgo hacia historias promocionales.

3.4.1. Industria, construcción y actividades de alto riesgo

En manufactura, minería, energía, transporte y construcción, las tecnologías observan proximidad, atmósferas, equipos, posturas y uso de protección. Su fortaleza es actuar cerca del peligro; su principal riesgo es añadir alarmas sin modificar causas. Un sistema que avisa cada aproximación a una zona puede revelar un diseño deficiente de circulación. La intervención sostenible separa personas y equipos antes de entrenar respuestas repetidas.

La construcción presenta cambios continuos de geometría, contratistas y tareas. Un mapa válido por la mañana puede quedar obsoleto. Los dispositivos requieren configuración ágil y responsabilidades compartidas. Las plataformas basadas en modelado de información pueden incorporar prevención desde el diseño, pero necesitan participación de proyectistas y ejecutores. Oliveira et al. (2023) encontraron oportunidades de herramientas digitales para prevención a través del diseño, junto con limitaciones de disponibilidad y desarrollo.

En maquinaria, las funciones automáticas se tratan como controles de ingeniería. Deben analizarse fallas, latencia, interferencia y estado seguro. La IA de visión puede complementar resguardos, no sustituirlos cuando estos son practicables. La suciedad, oclusión y cambios de iluminación demandan pruebas. Los trabajadores necesitan saber qué área cubre el sistema y qué ocurre si está degradado.

Los wearables en actividades peligrosas enfrentan compatibilidad con cascos, arneses, respiradores y ropa. Peso, calor y enganche pueden crear peligros. Un piloto debe incluir duración completa y tareas intensas. Mendes et al. (2026) señalan que gran parte de la evidencia permanece en evaluaciones controladas o de corto plazo; por ello, la aceptación inicial no demuestra sostenibilidad.

La alta rotación y subcontratación requieren inducción breve, multilingüe y verificable. Configurar perfiles individuales complejos puede ser inviable. La solución debe funcionar con cambios de personal sin bajar estándares. Los datos entre contratistas necesitan acuerdos claros, evitando que la organización principal pierda visibilidad o utilice el monitoreo para desplazar responsabilidad.

Las emergencias en actividades de alto riesgo muestran el límite de depender de interfaces ordinarias. Humo, ruido, evacuación o pérdida de energía modifican percepción y comunicación. Las funciones críticas deben tener alimentación de respaldo, señales distinguibles y un modo manual seguro. Los simulacros incluyen personas nuevas y contratistas, no únicamente equipos expertos que conocen el guion.

La analítica posterior no sustituye investigación. Los registros de sensor aportan una cronología, pero pueden omitir decisiones, metas conflictivas y condiciones no medidas. La reconstrucción combina datos, entrevistas y evidencia física.

Utilizar la plataforma como “testigo objetivo” puede dar una autoridad indebida a señales con incertidumbre.

3.4.2. Salud, servicios y nuevas modalidades de trabajo

En salud, las herramientas digitales conviven con sistemas clínicos, alarmas y decisiones sensibles. Pueden apoyar exposición, movilización, violencia o coordinación, pero también aumentar interrupciones. La implementación debe considerar carga de trabajo y seguridad del paciente. Una notificación de SST no puede competir sin jerarquía con una alarma clínica, ni utilizar información de pacientes fuera de su finalidad.

La participación del personal de primera línea resulta decisiva porque los flujos varían entre unidades. Una aplicación diseñada para consulta ambulatoria puede fallar en urgencias. La revisión de Baines et al. (2022) muestra que la innovación digital mejora cuando usuarios participan desde etapas tempranas; en servicios, la coproducción ayuda a reconocer interrupciones, privacidad y necesidades de soporte.

En oficinas y servicios, los riesgos pueden ser menos visibles: carga mental, sedentarismo, violencia, presión de clientes y disponibilidad continua. Las plataformas de productividad no deberían convertirse automáticamente en herramientas de salud. Medir pulsaciones o actividad para gestionar estrés puede individualizar un problema de carga y autonomía. La evaluación debe priorizar organización, demandas y apoyo.

El teletrabajo distribuye el lugar de trabajo y dificulta observar condiciones. Greer et al. (2023) documentaron desafíos y estrategias durante la expansión forzada del teletrabajo. Las soluciones preventivas incluyen evaluación ergonómica remota, canales de apoyo y acuerdos de disponibilidad, pero deben respetar el hogar y evitar vigilancia permanente. La OIT (2021) destaca para América Latina oportunidades y desafíos de conectividad, organización y regulación.

Las modalidades híbridas requieren continuidad entre espacios. La persona puede alternar oficina, hogar y movilidad, con exposiciones distintas. Un sistema debe permitir reportar contexto sin exigir monitoreo constante. Las políticas

definen pausas, desconexión, equipos y atención. La tecnología puede facilitar comunicación, pero no resolver por sí sola aislamiento o sobrecarga.

En plataformas digitales, la asignación algorítmica puede determinar ritmo, rutas e ingresos. La SST debe examinar cómo esas decisiones crean presión, fatiga o exposición vial. La transparencia sobre criterios y la posibilidad de revisión son controles relevantes. La OIT (2025) incluye la gestión algorítmica y las nuevas formas de trabajo entre los retos de la digitalización preventiva.

En atención sanitaria y social, el trabajo emocional y la violencia requieren canales discretos y respuesta real. Un botón de pánico aumenta confianza solo si la localización funciona y llega apoyo. Probarlo implica tiempos, zonas sin cobertura y protocolos con seguridad. Los registros deben proteger a pacientes y trabajadores, evitando que una herramienta de auxilio se transforme en seguimiento continuo.

Los servicios con atención al público suelen contar con alta diversidad lingüística y laboral. Las aplicaciones deben admitir relevos, rotación y dispositivos compartidos sin exponer datos del usuario anterior. El inicio de sesión, la higiene y la gestión de perfiles forman parte del diseño. Una solución que tarda varios minutos en activarse puede no utilizarse en periodos de alta demanda.

3.4.3. Entornos rurales y operaciones en territorios complejos

Los territorios rurales, amazónicos, montañosos, marítimos o fronterizos combinan distancia, conectividad intermitente, clima y acceso limitado a soporte. Una solución dependiente de nube puede fallar cuando más se necesita. El diseño debe priorizar autonomía local, almacenamiento, sincronización diferida y comunicaciones alternativas. “Sin datos” debe mostrarse como incertidumbre, no como ausencia de riesgo.

La logística modifica sostenibilidad. Baterías, calibración y repuestos pueden tardar días. Los equipos se seleccionan por reparabilidad, consumo y disponibilidad regional. Manuales sin conexión, diagnóstico local y componentes estandarizados reducen dependencia. La formación de personal del territorio resulta más efectiva que enviar soporte ocasional que desconoce la operación.

El ambiente exige pruebas reales. Humedad, polvo, altura, lluvia, salinidad y calor afectan sensores y pantallas. La protección física puede aumentar peso o temperatura. Los pilotos deben abarcar estaciones y rutas, no solo un día favorable. La conectividad satelital puede apoyar comunicaciones, pero su latencia, costo, visibilidad y energía necesitan evaluación.

La inclusión cultural y lingüística es parte de la seguridad. Comunidades y trabajadores locales pueden interpretar señales y riesgos de manera distinta. El diseño participativo debe reconocer autoridades, horarios, idiomas y conocimiento territorial. Extraer datos sin beneficio local reproduce desigualdad. Los acuerdos definen propiedad, acceso, finalidad y retorno de información.

En agricultura y trabajo disperso, localizar a una persona puede acelerar rescate, pero también crear vigilancia. La necesidad debe delimitarse por tarea y tiempo. Es posible activar seguimiento durante una operación aislada y eliminar trayectorias después del periodo definido. Los modos de emergencia requieren pruebas y protocolos sobre quién responde; un botón sin cobertura o centro de atención es una promesa vacía.

Las brechas digitales afectan adopción. La solución debe ofrecer interfaces simples, formación práctica y canales alternativos. La OMS (2022) ha advertido que el acceso a tecnologías digitales de salud no se distribuye de forma equitativa; el principio es aplicable a servicios preventivos en territorios con menor conectividad. Diseñar para la infraestructura ideal puede aumentar la diferencia entre centros y periferias.

La autonomía local debe acompañarse de escalamiento. Un equipo remoto necesita autoridad para detener, aislar o evacuar sin esperar conexión, y una ruta para solicitar apoyo especializado cuando sea posible. Los procedimientos definen decisiones que pueden tomarse localmente y recursos disponibles. Centralizar toda interpretación en una ciudad aumenta latencia y puede ignorar conocimiento territorial.

Los datos geográficos y comunitarios requieren protección adicional. Una trayectoria puede revelar lugares sensibles, comunidades o recursos. La publicación de mapas se agrega y consulta con actores locales. Los beneficios deben retornar mediante alertas, capacitación o mejoras, no limitarse a extraer

información para un centro corporativo. La gobernanza territorial es parte de la legitimidad del sistema.

3.4.4. Lo que enseñan los aciertos, las resistencias y los errores

Los aciertos suelen compartir un patrón: problema delimitado, participación temprana, piloto contextual, responsables claros y evaluación continua. La tecnología se integra con controles existentes y la organización acepta modificarla. El éxito no se expresa solo en uso, sino en una respuesta más oportuna, menor exposición o mejor funcionamiento de barreras. Documentar condiciones de éxito evita atribuir todo al dispositivo.

La resistencia puede proteger al sistema de una mala decisión. Un trabajador que retira un wearable quizá denuncia incomodidad, interferencia o desconfianza. Investigar la conducta produce información; sancionarla puede ocultarla. También existe resistencia por fatiga de cambio, falta de tiempo o experiencias fallidas. No toda oposición es razonable, pero ninguna debería descartarse sin comprender.

Los errores técnicos deben tratarse como incidentes de aprendizaje. Un falso negativo, pérdida de conexión o dato equivocado puede no causar daño y aun revelar una barrera débil. Se necesita un canal de reporte, clasificación, contención, investigación y comunicación. Los registros de versión permiten saber qué instalaciones están afectadas. Cuando el proveedor corrige, la organización valida en su contexto.

Los errores organizacionales son menos visibles: nadie responde, dos áreas suponen que la otra actúa o el indicador incentiva ocultamiento. Las pruebas de extremo a extremo y la revisión de eventos los hacen observables. El análisis evita buscar culpables y examina diseño, carga, autoridad, formación y prioridades. Una corrección que solo recuerda “estar atentos” suele ser insuficiente.

La retirada también genera aprendizaje. Una solución puede detenerse por bajo desempeño, costo, rechazo o cambio de proceso. Cerrar de manera ordenada exige controles alternativos, exportación y eliminación de datos, comunicación y

recuperación de competencias. Retirar no convierte el proyecto en fracaso si evita daño y documenta por qué el enfoque no funcionó.

EU-OSHA (2023b) destaca que los recursos de implementación —información, instrucciones, formación y orientación ergonómica— condicionan el funcionamiento de sistemas inteligentes. La innovación no termina con el despliegue; necesita mantenimiento técnico y social. Las reuniones de revisión, métricas de carga, auditorías de equidad y participación sostenida forman parte del producto preventivo.

Un registro de lecciones debe ser específico. En lugar de “mejorar capacitación”, señala qué grupo no comprendió qué función, bajo qué condición y qué cambio se probará. Cada lección se vincula con responsable y verificación. Las bases corporativas de conocimiento sirven si permiten buscar por peligro y contexto; una colección de presentaciones sin seguimiento rara vez cambia la práctica.

La comunicación de errores protege confianza cuando es rápida, proporcional y honesta. Se informa qué ocurrió, a quién puede afectar, qué conducta provisional adoptar y cuándo habrá actualización. Ocultar una falla para evitar rechazo suele amplificarlo. También se reconocen los aportes de quienes reportaron, reforzando que cuestionar la herramienta es parte de la prevención.

La secuencia que deja este capítulo es deliberadamente práctica: escuchar, evaluar preparación, codiseñar, probar, gobernar la decisión, coordinar la respuesta y aprender. Cada paso reduce una clase de incertidumbre. Ninguno garantiza por sí solo el resultado, pero juntos evitan que la organización confunda digitalización con prevención. La innovación llega al trabajo cuando se vuelve comprensible, discutible y accionable para quienes viven el riesgo, sin pedirles que compensen fallas de diseño ni renuncien a sus derechos.

Figura 3.

Monitoreo en Tiempo Real y Ecosistema Tecnológico

Capítulo IV: El futuro del trabajo seguro se construye con responsabilidad

El futuro del trabajo seguro se construye con responsabilidad

La innovación preventiva promete reconocer peligros antes, ampliar la cobertura de las mediciones y apoyar decisiones que durante años dependieron de información fragmentada; esa promesa no convierte a la tecnología en un actor neutral. Un sistema selecciona variables, clasifica situaciones y distribuye atención; por tanto, incorpora decisiones humanas acerca de qué riesgo importa, qué error se tolera y quién debe responder; cuando esas elecciones permanecen ocultas, la automatización puede crear una apariencia de objetividad que dificulta cuestionar sus resultados.

La responsabilidad comienza antes de elegir un algoritmo; surge al definir el problema, delimitar la finalidad, evaluar alternativas y decidir si la recolección de datos es proporcional. Continúa durante el diseño, la compra, la validación y el uso; permanece cuando el sistema se actualiza y también al retirarlo; ningún contrato, proveedor o modelo desplaza el deber de proteger a las personas. La inteligencia artificial (IA) puede apoyar el juicio preventivo, pero la organización conserva la obligación de asegurar condiciones de trabajo saludables y de responder cuando la herramienta falla.

El reto no es únicamente evitar daño tecnológico; también consiste en impedir que la innovación debilite controles existentes, aumente desigualdades o convierta la vigilancia en sustituto del rediseño. Fisher et al. (2023) señalan que la IA puede reducir o exacerbar inequidades en seguridad y salud en el trabajo (SST), según los datos, el contexto y la distribución de sus beneficios; la Organización Internacional del Trabajo (OIT, 2025) observa una tensión similar: automatización y monitoreo pueden reducir exposiciones, mientras la gestión algorítmica, la intensificación y las nuevas modalidades generan riesgos que exigen respuestas preventivas.

Este capítulo aborda la responsabilidad como una arquitectura de decisiones; examina primero la centralidad de las personas; después analiza sesgos, explicabilidad y atribución de responsabilidad. La confianza se estudia desde privacidad y ciberseguridad; a continuación se desarrollan reglas de gobernanza, participación, transparencia y rendición de cuentas. El cierre mira hacia

profesiones, competencias y sostenibilidad; la tesis que articula el recorrido es que el trabajo seguro del futuro no depende de cuánta tecnología se incorpore, sino de la calidad ética, técnica y organizacional con la que se gobierna.

4.1. Innovar sin perder de vista a las personas

La centralidad humana no significa colocar una interfaz amable sobre una decisión ya tomada; exige que finalidad, diseño y evaluación partan de la protección de la vida, la salud, la dignidad y los derechos. Una herramienta es centrada en las personas cuando responde a una necesidad legítima, reduce riesgo de forma demostrable y ofrece capacidad de comprender, cuestionar y corregir; la comodidad de la organización o la disponibilidad de datos no bastan para justificarla.

La jerarquía de controles continúa siendo el referente; si un peligro puede eliminarse o aislarse, un wearable que advierte a la persona ocupa una posición secundaria. La digitalización puede fortalecer controles de ingeniería mediante detección y parada, pero también desplazar la carga hacia el individuo; pedir que una persona responda continuamente a alertas de una máquina mal diseñada no es prevención avanzada; es dependencia de conducta ante una fuente que permanece.

La evaluación debe considerar beneficios y cargas; entre los beneficios se encuentran detección más oportuna, menor exposición, apoyo a rescate y mejor aprendizaje. Las cargas abarcan uso del dispositivo, interrupciones, ansiedad, datos personales, exclusión y posible intensificación; es frecuente que beneficios organizacionales —información, eficiencia o control— recaigan en una parte, mientras la incomodidad y la vigilancia recaen en otra. Hacer visible esta distribución permite negociar salvaguardas.

La prudencia también responde al estado de la evidencia; jetha et al. (2025) encontraron muy pocos estudios que evaluaran efectos de herramientas de IA sobre lesiones o enfermedades laborales. El-Helaly (2024) describe beneficios potenciales y desventajas relacionadas con privacidad, sesgo y dependencia; la organización no debería confundir un buen desempeño de laboratorio con efectividad preventiva sostenida.

La Recomendación sobre la Ética de la IA de la UNESCO sitúa derechos humanos, dignidad, transparencia, equidad, sostenibilidad y supervisión humana como principios de referencia (UNESCO, 2021); en SST, estos principios se traducen en decisiones concretas: limitar finalidad, involucrar trabajadores, evaluar impacto por grupos, documentar incertidumbre y mantener vías de revisión. La ética deja de ser una declaración cuando se convierte en requisitos, pruebas y responsabilidades.

La participación debe ocurrir durante todo el ciclo; quienes realizan el trabajo aportan conocimiento sobre variaciones, presiones y consecuencias que no aparecen en los conjuntos de datos. También identifican usos secundarios previsibles; un sistema fisiológico presentado como prevención puede terminar comparando rendimiento; una cámara de proximidad puede utilizarse para disciplina. Discutir estas posibilidades antes del despliegue permite prohibirlas técnica y normativamente.

La supervisión humana necesita condiciones reales; una persona no puede revisar una recomendación si recibe cientos de alertas, desconoce el modelo o teme contradecirlo. Autoridad, formación, tiempo e información son componentes del control; la capacidad de anular no debe ser meramente formal; se prueba en escenarios y se analizan discrepancias sin sancionar automáticamente.

El enfoque humano incluye a quienes suelen quedar fuera: contratistas, trabajadores de plataformas, migrantes, personas con discapacidad, pequeñas empresas y territorios con menor conectividad; fisher et al. (2023) advierten que los beneficios de la IA pueden distribuirse de forma desigual entre grupos, industrias, arreglos laborales y regiones. La innovación responsable pregunta desde el principio quién no está representado y qué alternativa tendrá. La evaluación centrada en las personas necesita indicadores propios; además del desempeño del modelo, se miden carga, comprensión, confianza calibrada, posibilidad de impugnación y efecto sobre autonomía. Una reducción del tiempo administrativo puede coexistir con mayor presión; una alerta precisa puede aumentar ansiedad; las métricas se combinan con entrevistas y observación, porque algunas consecuencias no aparecen en un tablero.

La reversibilidad es otro criterio; un piloto responsable puede detenerse sin dejar a la operación sin controles, conservar una ruta manual y eliminar datos recogidos. Las decisiones difíciles de revertir —por integración profunda, contratos largos o pérdida de competencias— requieren mayor evidencia antes de avanzar; diseñar una salida no expresa falta de compromiso; protege frente a incertidumbre. La centralidad humana se prueba cuando entra en conflicto con eficiencia; si un sistema aumenta productividad pero eleva exposición o reduce pausas, la organización debe corregirlo. Si una función preventiva depende de datos desproporcionados, se rediseña; los principios adquieren sentido precisamente cuando limitan una opción técnicamente posible.

4.2. Los dilemas éticos de la prevención algorítmica

La prevención algorítmica utiliza reglas o modelos para clasificar señales, estimar riesgos o recomendar acciones; el dilema ético no proviene de que una máquina “piense”, sino de que sus resultados influyen sobre personas y sistemas en condiciones de incertidumbre. Elegir una variable, una etiqueta o un umbral puede cambiar quién recibe protección, quién es observado y qué explicación se considera válida.

Un modelo optimiza una función, no el conjunto de valores de la organización; puede reducir falsas alarmas a costa de pasar por alto eventos en un grupo pequeño. Puede priorizar productividad y declarar “segura” una operación mientras no mide carga mental; la decisión ética consiste en definir qué daños se consideran, quién participa y cómo se resuelven conflictos. Las métricas técnicas son necesarias, pero no sustituyen esa deliberación.

La escala amplifica consecuencias; un criterio defectuoso aplicado por un supervisor afecta casos limitados y puede ser discutido; incorporado a una plataforma, se replica con velocidad y consistencia aparente. La homogeneidad no equivale a justicia si la regla inicial es sesgada; por ello se requieren evaluaciones antes y durante el uso, no solo una validación al comprar.

El contexto laboral añade asimetrías; el consentimiento individual puede ser insuficiente cuando rechazar una herramienta afecta empleo o asignación. La gobernanza colectiva, la negociación y la protección normativa resultan más

adecuadas para algunos usos; la ética no debe trasladar toda la carga a una casilla de aceptación.

Los dilemas pueden analizarse mediante escenarios; se describe la decisión, actores, beneficios, daños, incertidumbres, alternativas y grupos afectados. Después se examina qué ocurriría si el sistema falla, funciona demasiado bien o se usa con otra finalidad; este ejercicio revela riesgos secundarios: una detección de fatiga puede proteger y, a la vez, incentivar selección de quienes generan menos alertas.

La proporcionalidad relaciona intrusión y beneficio; un sistema de localización continua podría justificarse durante rescates o trabajo aislado, pero no necesariamente durante toda la jornada. La misma tecnología cambia de valoración según tarea, duración y salvaguardas; definir ventanas, zonas y eliminación reduce alcance sin perder función.

Los conflictos necesitan una instancia de resolución; el equipo técnico puede priorizar precisión, privacidad la minimización y operación la rapidez. Un comité interdisciplinario debe argumentar y registrar la decisión; la ética aplicada no elimina desacuerdo; evita que gane por defecto quien controla presupuesto o software.

4.2.1. Sesgos que pueden convertirse en nuevas formas de riesgo

El sesgo puede ingresar por definición del problema, selección de datos, medición, etiquetas, modelado, umbral e implementación; no siempre es una intención discriminatoria. Un sensor calibrado en condiciones limitadas puede rendir peor con otros cuerpos o equipos; una base de incidentes puede reflejar subregistro; una etiqueta de “acto inseguro” puede ocultar fallas de organización; el algoritmo aprende relaciones presentes en los datos, incluidas sus ausencias y desigualdades.

La representatividad es una primera prueba; si un modelo de fatiga se entrenó con trabajadores jóvenes de un sector, no debería generalizarse a poblaciones diferentes sin validación. Edad, sexo, discapacidad, idioma, tipo de contrato, turno y región pueden modificar exposición o desempeño; recoger estas

variables para auditar equidad puede ser legítimo, pero aumenta sensibilidad de los datos y requiere finalidad, minimización y control.

El sesgo de medición aparece cuando una variable proxy reemplaza el fenómeno; ausentismo puede utilizarse como indicador de salud, aunque también refleja responsabilidades de cuidado, transporte o políticas. Velocidad de tarea puede confundirse con conducta segura, ignorando complejidad; en modelos de riesgo, una variable fácil de obtener puede dominar porque está disponible, no porque sea causal.

Las etiquetas históricas son especialmente delicadas; si las investigaciones atribuyeron incidentes a “error humano” de manera sistemática, el modelo reproducirá ese enfoque. La revisión de casos debe incorporar mecanismos de daño, exposiciones, barreras y factores organizacionales; un comité multidisciplinario puede examinar muestras y desacuerdos; la incertidumbre en la etiqueta se conserva en lugar de forzar una certeza falsa.

Fisher et al. (2023) proponen entender la equidad de SST a lo largo del diseño y la adopción de IA. Auditar solo la exactitud global oculta diferencias; sensibilidad, falsos positivos, calibración y consecuencias deben examinarse por grupos relevantes, siempre que el tamaño permita interpretación y se proteja privacidad. Una diferencia estadística activa investigación; no prueba por sí sola discriminación ni autoriza etiquetar a la población.

La mitigación puede actuar sobre datos, modelo y decisión; incluye ampliar representación, corregir mediciones, cambiar variables, ajustar umbrales o introducir revisión. Ninguna técnica resuelve por sí misma una definición injusta; los criterios de equidad pueden entrar en tensión: igualar falsos negativos puede alterar otros resultados. La organización debe documentar qué criterio eligió, por qué y con qué participación.

El sesgo también aparece después del modelo; una alerta idéntica puede recibir respuestas distintas según área o contrato. Si una planta tiene recursos y otra no, el sistema amplía la brecha; evaluar impacto exige seguir la cadena hasta la acción. La justicia preventiva se observa en acceso efectivo a controles, no solo en predicciones. La deriva puede crear sesgo nuevo; cambios en población, equipo, clima o reporte alteran relaciones. Un modelo inicialmente equilibrado

puede deteriorarse de forma desigual; el monitoreo compara distribuciones y errores por periodo; las alertas de deriva conducen a revisión, no a reentrenamiento automático con datos recientes. Estos pueden contener un problema emergente.

Los grupos pequeños plantean una tensión entre auditoría y privacidad; agregar demasiado oculta diferencias; desagregar puede identificar. Se pueden combinar periodos, utilizar revisión cualitativa o recurrir a auditoría independiente con acceso controlado; la ausencia de una cifra pública no debe convertirse en ausencia de evaluación. La documentación incluye la historia de exclusiones; debe indicar qué poblaciones no participaron, qué condiciones no se probaron y en qué dominio no se autoriza el uso. Una ficha que solo enumera fortalezas incentiva generalización; los límites forman parte del desempeño y deben acompañar cada versión.

4.2.2. Explicar las decisiones de la inteligencia artificial

Explicar no consiste en mostrar código ni producir una narración convincente; una explicación útil responde a la necesidad del destinatario. El desarrollador requiere información para depurar; el especialista de SST, variables y límites; el supervisor, fundamento de la alerta; el trabajador, qué datos influyeron y cómo solicitar revisión; una misma salida necesita capas de información.

La interpretabilidad describe cuánto puede comprenderse el mecanismo del modelo; la explicabilidad incluye métodos que presentan razones sobre un sistema complejo; las explicaciones posteriores pueden ser aproximaciones y variar. Deben identificarse como tales; un gráfico de importancia no demuestra causalidad, y una explicación local no describe el comportamiento general.

El National Institute of Standards and Technology considera explicabilidad e interpretabilidad entre las características de una IA confiable, junto con validez, seguridad, resiliencia, privacidad, transparencia y equidad (Tabassi, 2023); el marco organiza la gestión en gobernar, mapear, medir y gestionar. Para explicar una alerta primero debe conocerse el contexto, la población, los datos y el uso autorizado.

La explicación mínima de una alerta incluye condición detectada, fuente, tiempo, ubicación, nivel de confianza, variables relevantes y acción esperada; en una decisión con efectos sobre la persona se añade base, alternativas, responsable humano y mecanismo de impugnación. Frases genéricas como “el sistema identificó un patrón” no permiten revisar.

La transparencia debe ser proporcionada a la criticidad; un umbral simple puede documentarse por completo; un modelo complejo requiere ficha técnica, datos, métricas, limitaciones y pruebas. Los secretos comerciales no deberían impedir que la organización comprenda riesgos suficientes para cumplir su deber; si el proveedor no permite auditoría ni ofrece evidencia, la incertidumbre forma parte de la decisión de compra.

Las explicaciones se prueban con usuarios; se evalúa si interpretan prioridad, incertidumbre y conducta. Una interfaz puede ser técnicamente correcta y generar conclusiones equivocadas; la precisión verbal importa: “riesgo alto” no significa que el evento ocurrirá ni que la persona sea peligrosa. Conviene distinguir observación, inferencia y recomendación. Existe un riesgo de explicación ornamental; una interfaz puede presentar colores y factores para aumentar confianza sin revelar límites. La explicación debe permitir detectar error y no solo persuadir; por eso se conecta con evidencia, versión y registro de decisiones. Cuando un resultado no puede explicarse al nivel requerido para su impacto, el uso puede ser inaceptable.

Las explicaciones contrafactuales pueden mostrar qué cambio habría modificado el resultado: “la alerta no se habría activado si la concentración permanecía por debajo del umbral”; son útiles cuando las variables representan condiciones controlables. Son problemáticas si sugieren que una persona cambie edad, salud o identidad; la selección de factores debe evitar trasladar responsabilidad a características no modificables.

En modelos generativos, una respuesta fluida puede ocultar invención o variabilidad; si se usan para resumir incidentes o proponer controles, las fuentes y el texto original deben permanecer disponibles. No se acepta una recomendación por calidad retórica; las salidas se tratan como borradores sujetos a revisión y se prohíbe introducir datos personales en servicios no

autorizados. La explicación debe conservarse junto con la decisión; si el modelo cambia, una explicación reproducida después podría diferir. Registrar versión, entrada y resultado permite investigar; para sistemas críticos, la trazabilidad temporal es parte de la seguridad, no una función de auditoría opcional.

4.2.3. Responsabilidad cuando la tecnología se equivoca

Los errores adoptan formas diferentes: falso negativo, falsa alarma, recomendación inapropiada, falla de comunicación o acción incorrecta; la responsabilidad depende de la cadena. El proveedor pudo entrenar con datos insuficientes; la organización configuró mal; mantenimiento omitió calibración; la interfaz indujo error; la dirección no asignó respuesta; reducir todo a quien presionó un botón impide aprender.

Una matriz de responsabilidades define propietario del sistema, del modelo, del dato, del proceso y de la decisión; también soporte, seguridad, privacidad y representación laboral. Cada rol tiene autoridad y obligación; el propietario del proceso responde por integrar la herramienta; el área técnica por disponibilidad; SST por criterios preventivos; el proveedor por compromisos contractuales. La dirección conserva responsabilidad sobre recursos y gobernanza.

La automatización no crea un vacío; incluso cuando una parada es automática, personas diseñaron lógica, límites y recuperación. Las funciones críticas necesitan análisis de peligros, validación independiente y estados seguros; el registro debe permitir reconstruir datos, versión, salida y acción. Sin trazabilidad, investigar resulta especulativo.

El error debe comunicarse y contenerse; se identifica a quién puede afectar, se suspende o limita el sistema y se activa un control alternativo. Después se investiga causa técnica y organizacional; una corrección de software no basta si la organización carecía de supervisión. Los trabajadores reciben información clara sobre alcance y conducta provisional.

El Reglamento de IA de la Unión Europea adopta un enfoque basado en riesgo y clasifica como de alto riesgo determinados sistemas vinculados con empleo y gestión de trabajadores (Unión Europea, 2024); su aplicación es gradual y depende del caso; no constituye una norma universal para América Latina, pero

ilustra obligaciones de gestión, documentación, supervisión y monitoreo. Las organizaciones deben revisar la legislación de cada jurisdicción.

Los contratos necesitan criterios de desempeño, notificación de incidentes, cambios, auditoría, ciberseguridad, conservación y salida; una cláusula que exonera al proveedor no transforma una herramienta insegura en aceptable. La organización debe disponer de competencia para evaluar evidencias; la dependencia tecnológica no es defensa frente al daño.

La cultura justa distingue error, negligencia y conducta deliberada; si una persona sigue una recomendación razonable que luego falla, atribuirle culpa desalienta el uso y el reporte. Si alguien anula una alarma, se investiga contexto: pudo reconocer un falso positivo; los registros apoyan aprendizaje, no una sanción automática.

La reparación tiene varias dimensiones; puede requerir atención de salud, corrección de datos, restitución de una decisión laboral, compensación, disculpa e información sobre cambios. Corregir el modelo evita recurrencia, pero no resuelve el daño ya causado; los canales deben permitir que la persona afectada conozca el resultado de la revisión.

Los incidentes cercanos también se investigan; una alerta no entregada que fue detectada por otro control aporta evidencia sobre dependencia. Clasificar solo daños consumados pierde oportunidades; el sistema de reporte integra incidentes algorítmicos con la gestión de SST, privacidad y ciberseguridad, evitando tres investigaciones desconectadas.

La organización debe ensayar la asignación de responsabilidad antes del evento; los ejercicios plantean una salida incorrecta, proveedor indisponible y datos incompletos. Se observa quién puede suspender, qué control alternativo existe y cómo se comunica; las ambigüedades corregidas durante un simulacro evitan improvisación bajo presión.

4.3. La confianza también necesita protección

La confianza no surge de pedir que las personas crean en la tecnología; se construye mediante desempeño, límites verificables y capacidad de reparación. Un sistema confiable puede fallar, pero detecta la falla, informa y conserva una

ruta segura; la confianza ciega es peligrosa; la desconfianza permanente impide beneficios. El objetivo es una confianza calibrada.

Privacidad y ciberseguridad son condiciones preventivas; la primera protege control y uso legítimo de información; la segunda preserva confidencialidad, integridad y disponibilidad. En sistemas conectados, una intrusión puede alterar una alarma o detener un control, convirtiendo un problema digital en riesgo físico; del mismo modo, un programa técnicamente seguro puede violar privacidad si recoge más de lo necesario.

La confianza también depende de coherencia institucional; si los datos recogidos para prevención se usan después para productividad, la promesa inicial se rompe aunque el uso sea técnicamente permitido por una política amplia. La limitación de finalidad y la participación protegen la relación; los cambios deben comunicarse y evaluarse antes, no después.

La competencia percibida influye; una organización que no calibra sensores o tarda en corregir errores difícilmente obtiene confianza mediante campañas. Publicar resultados de pruebas, tiempos de respuesta y mejoras ofrece evidencia; también deben reconocerse límites: afirmar seguridad absoluta prepara una ruptura ante el primer incidente.

La confianza es relacional y puede variar entre actores; un trabajador puede confiar en el dispositivo y no en quien accede a los datos; un supervisor puede confiar en la alerta y no en el proveedor. Evaluar estas dimensiones orienta controles; no conviene resumir todo en una única pregunta de aceptación.

La protección frente a represalias resulta esencial; si cuestionar un resultado afecta evaluación, los errores permanecen ocultos. Los canales confidenciales, la participación colectiva y el seguimiento de quejas permiten corregir; la confianza aumenta cuando se demuestra que reportar produce mejora y no castigo.

4.3.1. Privacidad de los datos personales y biométricos

Los sistemas preventivos pueden registrar ubicación, voz, imagen, postura, frecuencia cardiaca, temperatura o actividad; algunos datos son identificables; otros permiten inferencias sobre salud, conducta o relaciones. Lo biométrico no

se reduce a huella o rostro: según el tratamiento y la jurisdicción, características fisiológicas o conductuales pueden requerir protección reforzada; la organización debe clasificar antes de recoger.

La minimización pregunta qué dato es imprescindible, con qué resolución y durante cuánto tiempo; para una alerta local quizá basta procesar en el dispositivo y no conservar. Para analizar una zona puede agregarse por tarea; guardar trayectorias y señales continuas “por si acaso” aumenta riesgo y costo. Cada campo debe vincularse con una finalidad y un plazo. El consentimiento laboral tiene límites por la desigualdad de poder; la base jurídica dependerá del país y del uso. Aun cuando exista fundamento, se requiere información comprensible, proporcionalidad y derechos; no debe presentarse una aceptación obligatoria como elección libre. La consulta colectiva y las evaluaciones de impacto complementan requisitos legales.

La separación de usos reduce abuso; los datos preventivos no deben fluir automáticamente hacia recursos humanos, productividad o seguros. Los accesos se asignan por rol, con registros y revisión; los identificadores se sustituyen cuando es posible, aunque la seudonimización no elimina la capacidad de reidentificar. La anonimización requiere análisis real, especialmente en grupos pequeños.

Los hallazgos incidentales necesitan protocolo; un wearable puede detectar una señal que sugiere un problema sin haber sido diseñado para diagnosticar. Informar sin validación puede causar ansiedad; ignorar puede ser problemático; antes del piloto se define qué se considera hallazgo, quién valida, cómo se comunica y qué apoyo existe. El algoritmo no debe declarar diagnósticos ni aptitud fuera de su autorización.

La obra Salud digital 4.0 aborda privacidad, trazabilidad, sesgos e interoperabilidad en el contexto sanitario latinoamericano (Rodríguez-Lindao et al., 2026); aunque el marco clínico no es idéntico al ocupacional, muestra una tensión compartida: el valor analítico crece con integración, mientras el riesgo aumenta cuando se difuminan finalidades. La gobernanza debe avanzar al mismo ritmo que la capacidad de combinar datos.

Los derechos operativos incluyen conocer, acceder, corregir cuando corresponda y cuestionar decisiones; la interfaz o un canal alternativo debe permitir ejercerlos sin conocimiento técnico. Las solicitudes se atienden dentro de plazos definidos; un proveedor en la nube no debería convertir el derecho en un trámite imposible. La eliminación es parte del ciclo; al terminar la finalidad, el dato se borra de sistemas, copias y dispositivos según políticas verificables. Los modelos pueden conservar información derivada, lo que exige considerar si retirar registros requiere reentrenar; los contratos especifican devolución y destrucción. La retención indefinida por conveniencia contradice minimización.

La evaluación de impacto sobre privacidad comienza antes de recolectar y se actualiza con cambios; describe flujo, actores, riesgos y medidas. Pregunta si existe una alternativa menos intrusiva y qué ocurriría ante filtración o inferencia; su calidad depende de incorporar a trabajadores y especialistas, no de completar un formato después de la compra. Los datos biométricos pueden adquirir valor futuro no previsto; una señal recogida para estrés térmico podría utilizarse para inferir salud. Limitar acceso no basta si se conserva en formato reutilizable; procesamiento en el borde, extracción de la característica necesaria y descarte de señal bruta pueden reducir riesgo. La arquitectura expresa así una decisión ética.

La portabilidad y localización de datos importan en servicios transnacionales; la organización debe conocer dónde se procesan, qué subcontratistas intervienen y qué ocurre al terminar. Las leyes varían; por tanto, se requiere asesoría competente; el capítulo ofrece principios de gobernanza y no reemplaza la evaluación jurídica de cada país. La privacidad colectiva también merece atención; aunque se eliminen nombres, un análisis puede etiquetar un área o colectivo como “problemático” y producir consecuencias. La revisión evalúa cómo se presentarán resultados y quién interpretará; agregar no elimina todo daño cuando el grupo es identificable.

4.3.2. Ciberseguridad en sistemas preventivos conectados

Un sistema conectado amplía la superficie de ataque mediante sensores, aplicaciones, puertas de enlace, nube y proveedores; las amenazas incluyen credenciales robadas, software vulnerable, manipulación de datos, denegación

de servicio y actualización comprometida. En SST, integridad y disponibilidad pueden ser tan críticas como confidencialidad; una alarma alterada o ausente afecta decisiones físicas. El Cybersecurity Framework 2.0 organiza resultados en gobernar, identificar, proteger, detectar, responder y recuperar (Pascoe et al., 2024); su carácter flexible permite adaptarlo a distintos tamaños. Para sistemas preventivos, gobernar implica vincular riesgo cibernético con seguridad operacional, asignar responsables y considerar cadena de suministro.

El inventario es un primer control: dispositivo, versión, propietario, conexión, datos y criticidad; equipos olvidados no reciben actualizaciones. La segmentación separa redes operacionales y administrativas; el mínimo privilegio limita accesos; la autenticación protege cuentas y dispositivos; las contraseñas predeterminadas deben eliminarse y las comunicaciones críticas cifrarse cuando sea apropiado. Las actualizaciones requieren equilibrio; no instalar parches deja vulnerabilidades; desplegarlos sin prueba puede interrumpir. Se evalúan en entorno controlado, se programa ventana y se conserva recuperación; el proveedor debe informar soporte y fin de vida. Un sensor funcional que ya no recibe seguridad puede ser inaceptable.

La detección debe distinguir falla, ataque y variación operacional; registros sincronizados permiten investigar. Las alertas de ciberseguridad necesitan su propia priorización para no saturar; los equipos de tecnología, operación y SST comparten escenarios: pérdida de conectividad, datos imposibles, comandos no autorizados o indisponibilidad de nube. La respuesta prepara modos degradados; si el sistema cae, se conserva una barrera alternativa y se comunica la pérdida de cobertura. Nunca debe mostrarse “sin riesgo” cuando no hay datos; para funciones críticas pueden requerirse redundancia, operación local o parada segura. Los simulacros prueban recuperación y decisiones manuales.

La cadena de suministro es central; bibliotecas, firmware, servicios y mantenimiento introducen dependencias. La compra examina prácticas del proveedor, divulgación de vulnerabilidades, autenticación, registro, actualizaciones y acceso remoto; las credenciales de mantenimiento se controlan y revocan. El tamaño del proveedor no garantiza seguridad. El factor humano no se reduce a capacitación contra phishing; interfaces complejas,

permisos excesivos y presión crean condiciones para errores. El diseño seguro facilita la conducta correcta; los reportes se reciben sin culpa automática. La ciberseguridad debe proteger el trabajo, no convertirse en vigilancia adicional.

La criticidad de cada activo orienta prioridad; un portal de capacitación y un sistema de parada no requieren el mismo tiempo de recuperación. El análisis considera impacto sobre personas, proceso y ambiente; las copias de seguridad se prueban; una copia nunca restaurada es una expectativa, no un control. El acceso remoto de proveedores debe activarse por necesidad, limitarse en tiempo y registrarse; las conexiones permanentes amplían riesgo. Las tareas de mantenimiento se coordinan con operación para evitar cambios durante estados críticos; al terminar el contrato, credenciales y certificados se revocan.

La respuesta a ransomware o indisponibilidad incluye decisiones físicas; ¿Puede continuar el proceso? ¿Qué monitoreo manual existe? ¿Cómo se informa a trabajadores? las respuestas no deben quedar solo en el plan de tecnología. SST participa en análisis de impacto y en criterios para parada y retorno. La recuperación verifica integridad antes de reactivar; restaurar comunicación no demuestra que umbrales, firmware y datos sean correctos. Se comparan configuraciones con una base conocida y se prueban alarmas; el retorno gradual permite observar anomalías. Las lecciones actualizan arquitectura, formación y contratos.

4.4. Gobernar la tecnología para cuidar mejor

Gobernar es establecer cómo se toman, documentan y revisan decisiones; una política general de IA no reemplaza la gobernanza de cada caso. El nivel de control depende de daño potencial, alcance, autonomía, datos y reversibilidad; un tablero agregado requiere menos garantías que un sistema que detiene maquinaria o influye sobre empleo.

El inventario de casos de uso permite conocer qué herramientas existen, quién las posee y qué datos utilizan; la IA incorporada en equipos puede pasar inadvertida; los proveedores pueden actualizar funciones. El registro incluye propósito, versión, población, métricas, riesgos, controles, incidentes y fecha de revisión; sin inventario no hay supervisión consistente.

El marco de NIST propone un ciclo de gobernar, mapear, medir y gestionar (Tabassi, 2023); gobernar crea cultura y responsabilidades; mapear comprende contexto e impactos; medir evalúa; gestionar prioriza y actúa. Las funciones son continuas; medir sin capacidad de detener convierte la auditoría en observación.

La gobernanza también define límites; algunos usos pueden prohibirse por desproporción: reconocimiento emocional no validado, monitoreo continuo para disciplina o diagnóstico fuera de competencia. Otros se autorizan con condiciones; las reglas deben ser comprensibles y aplicables a compras, desarrollos internos y pruebas gratuitas.

La clasificación por riesgo ayuda a asignar esfuerzo; se valoran gravedad, escala, autonomía, sensibilidad, grupos y posibilidad de reversión. Un sistema de bajo riesgo puede seguir un proceso ligero; uno alto requiere validación independiente, evaluación de impacto y monitoreo intensivo; la categoría se revisa si cambia la finalidad. El comité de gobernanza necesita mandato, composición y frecuencia; incluye dirección, SST, tecnología, privacidad, ciberseguridad, factores humanos y representación laboral. Puede invitar expertos; su función es decidir casos y revisar cartera; no administra cada alerta. Las actas registran razones y conflictos de interés.

La gobernanza internacional debe distinguir mínimos comunes y exigencias locales; una organización puede adoptar principios globales de dignidad, seguridad y transparencia y ajustar procedimientos a la ley. Aplicar el estándar menos protector de todas las sedes crea inequidad; el objetivo es coherencia con adaptación, no uniformidad ciega. Los principios de diseño publicados por EU-OSHA (2025) refuerzan la integración de requisitos humanos, organizacionales y técnicos en sistemas digitales de SST. Estas orientaciones no reemplazan normas locales, pero ayudan a transformar valores generales en preguntas sobre participación, datos, uso y evaluación durante el ciclo de vida.

4.4.1. Responsabilidades compartidas y reglas claras

La responsabilidad compartida no significa responsabilidad difusa; dirección, SST, tecnología, privacidad, ciberseguridad, salud ocupacional, compras, proveedores y trabajadores aportan funciones distintas. Una matriz puede indicar quién ejecuta, aprueba, consulta e informa; cada riesgo crítico debe tener un

propietario con autoridad y recursos. Las puertas de decisión ordenan el ciclo: aprobación del problema, datos, prototipo, piloto, despliegue, cambio y retiro; la evidencia aumenta con el impacto. Antes del piloto se revisa finalidad y privacidad; antes del despliegue, desempeño y respuesta; antes de automatizar, seguridad funcional y supervisión; las excepciones requieren justificación y plazo.

Las reglas de datos abarcan procedencia, calidad, acceso, retención y transferencia; las de modelo cubren validación, métricas, umbrales, deriva y actualización. Las operacionales asignan destinatario, acción y cierre; las humanas garantizan información, participación, accesibilidad y revisión. Integrarlas evita que cada área suponga que otra resolvió el riesgo. La compra debe evaluarse con criterios de SST. Una demostración comercial no prueba funcionamiento contextual; se solicitan datos de validación, limitaciones, grupos, tasa de error, ciberseguridad y soporte. Las afirmaciones se prueban en piloto; el contrato condiciona cambios y permite auditoría suficiente.

Los sistemas heredados requieren atención; una herramienta previa a la política puede tener datos y dependencias invisibles. Se inventaría y evalúa por prioridad; no es realista corregir todo a la vez, pero las funciones críticas no deberían quedar exentas por antigüedad. Los planes incluyen migración y controles temporales. La documentación debe estar viva; fichas, procedimientos y evaluaciones se actualizan con versiones. Los cambios pequeños pueden alterar desempeño; un registro de decisiones explica por qué se aceptó un riesgo y cuándo revisar. La documentación útil permite operar e investigar; no se limita a proteger jurídicamente.

La preparación de incidentes define notificación, contención, investigación y reparación; incluye daños a seguridad, privacidad, equidad y derechos. Un resultado sesgado puede ser incidente aunque no exista lesión; los canales deben permitir reportes de trabajadores y terceros. Las lecciones se comparten sin exponer datos personales. La gestión de cambios determina cuándo revalidar; nuevos datos, variables, umbrales, interfaz, proveedor o población pueden alterar el riesgo. Los cambios urgentes se documentan y revisan

después; las actualizaciones automáticas se restringen en sistemas críticos. Cada versión tiene fecha de entrada y plan de reversión.

Los indicadores de gobernanza examinan calidad, no solo cantidad; contar políticas o cursos puede dar una imagen favorable sin probar funcionamiento. Resultan más útiles el porcentaje de casos con propietario, incidentes cerrados con verificación, cambios revalidados y reclamaciones resueltas; la dirección recibe tendencias y decisiones pendientes. El retiro es una puerta formal; se define por obsolescencia, bajo desempeño, daño, costo o cambio de necesidad. El plan mantiene controles alternativos, conserva evidencias necesarias, elimina datos y recupera competencias; los usuarios conocen la fecha y la nueva ruta. Dejar una herramienta abandonada y conectada crea riesgo.

4.4.2. Participación, transparencia y rendición de cuentas

La participación aporta legitimidad y conocimiento; los trabajadores deben intervenir en definición, pruebas, evaluación y cambios, con tiempo e información. La consulta tardía sobre una decisión cerrada no es participación; los comités de SST o representación colectiva ofrecen continuidad, pero deben incluir grupos afectados. La transparencia tiene varios objetos: existencia del sistema, finalidad, datos, lógica general, responsables, riesgos y derechos; no exige publicar secretos o datos sensibles. Exige revelar lo necesario para comprender y cuestionar; la opacidad contractual no debería trasladarse a la persona afectada.

La rendición de cuentas añade consecuencias; un responsable debe explicar decisiones, corregir y reparar. Publicar una política sin evidencia no basta; indicadores pueden incluir cobertura de auditorías, incidentes, desempeño por grupos, anulaciones, tiempos de respuesta y cierres. Las métricas deben evitar incentivos de ocultamiento. Las evaluaciones de impacto organizan preguntas antes de usar: necesidad, proporcionalidad, actores, datos, riesgos, alternativas y salvaguardas; se actualizan con cambios. La Recomendación de UNESCO propone herramientas de preparación e impacto para trasladar principios a práctica (UNESCO, 2021); en SST, la evaluación se integra con el análisis de riesgos laborales y de datos.

La auditoría puede ser interna o independiente según criticidad; revisa evidencia, no solo cumplimiento documental. Pruebas reproducibles, muestras y entrevistas muestran operación real; los auditores necesitan acceso suficiente y competencia interdisciplinaria. La independencia se protege evitando que el equipo evaluado controle conclusiones.

Los mecanismos de impugnación deben ser accesibles; la persona conoce una decisión, solicita explicación y obtiene revisión humana. Los plazos y resultados se documentan; impugnar no puede generar represalia. Las recurrencias alimentan mejoras del sistema. La comunicación pública o interna debe evitar exageraciones; decir que la IA “evita accidentes” sin evidencia crea confianza indebida. Se presentan propósito, alcance, desempeño y límites; los errores se comunican oportunamente con acciones provisionales. La honestidad ante fallas sostiene más confianza que una imagen de infalibilidad.

La rendición también alcanza efectos ambientales y sociales; infraestructura, dispositivos y cómputo consumen energía y materiales; la adquisición puede depender de cadenas laborales opacas. La innovación responsable evalúa ciclo de vida, reparabilidad, duración y disposición; un beneficio preventivo no elimina otras obligaciones. La transparencia hacia trabajadores debe ser periódica; un aviso inicial pierde vigencia cuando cambian reglas. Informes breves pueden comunicar qué sistemas operan, qué datos usan, incidentes y mejoras; se evitan detalles que comprometan seguridad. La información se ofrece en formatos e idiomas accesibles.

La participación en auditorías aporta evidencia de uso real; entrevistas confidenciales y observación pueden revelar rutas paralelas, falsas alarmas o usos secundarios. Los trabajadores no son responsables de validar estadística, pero sí conocen impacto; sus aportes se contrastan y reciben devolución. La rendición de cuentas de la dirección es necesaria cuando metas productivas contradicen controles; un comité técnico no puede resolver incentivos definidos arriba. Los riesgos y decisiones se elevan con claridad; aceptar un riesgo implica señalar responsable, fundamento, plazo y salvaguarda, nunca trasladarlo silenciosamente a quien ejecuta.

4.5. Una mirada hacia los próximos escenarios del trabajo

Los próximos escenarios no dependen de una sola tecnología; IA generativa, robótica, sensores, realidad extendida, plataformas y gemelos digitales convergerán en procesos. La interacción crea beneficios y fallas emergentes; un modelo puede recomendar, un gemelo simular y un robot ejecutar; la trazabilidad debe atravesar la cadena. La incertidumbre exige vigilancia prospectiva; la organización identifica señales, escenarios y capacidades, no predice una fecha exacta. Pregunta qué tareas cambian, qué exposiciones se eliminan, cuáles aparecen y quién queda fuera; los pilotos se diseñan reversibles. La anticipación no justifica desplegar sin evidencia.

La automatización transformará autonomía, identidad y competencias; puede retirar personas de tareas peligrosas y aumentar supervisión o aislamiento. La evaluación de SST debe incluir factores psicosociales, carga cognitiva y ritmo; howard (2022) advierte sobre un “taylorismo digital” capaz de intensificar trabajo y erosionar autonomía. La regulación evolucionará y será desigual entre países; las organizaciones internacionales pueden orientar, pero cada jurisdicción define obligaciones. La gobernanza interna debe cumplir la ley y sostener principios consistentes cuando opera en varios territorios, evitando aplicar menor protección donde las reglas son débiles.

La IA generativa puede modificar documentación, capacitación y análisis de narrativas; su capacidad para sintetizar acelera tareas, mientras las alucinaciones, fugas y dependencia exigen control. Los contenidos de seguridad necesitan fuentes, revisión y versionado; un procedimiento no debe publicarse desde una salida sin validación profesional. El perfil de IA generativa del NIST organiza riesgos como confabulación, privacidad, seguridad de la información, contenido dañino y dependencia humano–máquina (Autio et al., 2024). En SST, su uso requiere límites más estrictos cuando la salida influye en una emergencia, una investigación o un control crítico.

La robótica móvil y colaborativa desplazará fronteras entre zona humana y automática; la evaluación deberá considerar comportamientos emergentes, aprendizaje y actualizaciones. Sensores de proximidad no sustituyen diseño seguro; la aceptación dependerá de previsibilidad y capacidad de detener. El

cambio climático interactuará con digitalización; sensores y modelos ayudarán a anticipar calor, humo o eventos extremos, pero conectividad y energía pueden fallar durante crisis. Los sistemas deben ser resilientes y accesibles; la sostenibilidad no es un apartado separado de la seguridad futura.

4.5.1. Profesiones y capacidades para la prevención del futuro

El profesional de SST necesitará comprender datos, algoritmos y ciberseguridad sin convertirse necesariamente en programador; debe formular preguntas, interpretar métricas, reconocer sesgos y conversar con especialistas. Las competencias técnicas se integran con higiene, ergonomía, medicina, factores humanos y gestión. La alfabetización de datos incluye procedencia, calidad, incertidumbre, asociación y causalidad; también saber cuándo un resultado no es suficiente. Leer una curva o una matriz de confusión ayuda a discutir umbrales; la capacidad más importante puede ser traducir desempeño estadístico a consecuencias humanas. La gobernanza ética requiere analizar finalidad, proporcionalidad, equidad y derechos; el profesional debe facilitar participación y comunicar incertidumbre. No basta aplicar una lista; los dilemas involucran valores en conflicto y necesitan deliberación documentada. La formación debe incluir casos y simulaciones.

La ciberseguridad se vuelve competencia compartida; SST debe reconocer cuándo una falla digital afecta barreras y participar en respuesta. El especialista de seguridad informática necesita comprender estados físicos seguros; ejercicios conjuntos crean lenguaje común. Pascoe et al. (2024) enfatizan que la gobernanza de ciberseguridad se vincula con riesgo empresarial. Los roles emergentes pueden incluir auditor de algoritmos, responsable de gobernanza, especialista en factores humanos digitales y gestor de datos de SST. En organizaciones pequeñas, estas funciones se distribuyen. Las redes sectoriales y servicios compartidos pueden aportar capacidad sin crear puestos completos.

La formación de trabajadores también cambia; deben entender qué hace la herramienta, cómo reconocer falla, qué datos usa y cómo cuestionar. La alfabetización en IA no es aprender marcas; es desarrollar juicio; los programas se adaptan por tarea, idioma y acceso. La práctica supera una presentación anual. La competencia colectiva importa; un experto aislado no compensa

procesos débiles. Equipos multidisciplinarios revisan casos y mantienen conocimiento cuando alguien se va; las decisiones y pruebas se documentan. La organización reserva tiempo para aprendizaje y actualización, evitando depender enteramente del proveedor.

Las universidades y programas profesionales deberán integrar ética de datos, factores humanos y ciberseguridad con práctica de SST. Los ejercicios pueden simular un sistema sesgado, una alarma incomprensible o un ataque. Evaluar no solo conocimiento, sino capacidad para detener y argumentar, prepara para decisiones reales. La contratación de perfiles técnicos no elimina la necesidad de traducción; científicos de datos deben comprender mecanismos de daño; profesionales de SST, supuestos del modelo. Los equipos crean vocabularios y criterios; las revisiones conjuntas evitan que “precisión” signifique cosas distintas para quien desarrolla y quien protege.

El liderazgo necesita alfabetización suficiente para no delegar ciegamente; debe preguntar por evidencia, límites, grupos y control alternativo. La dirección no tiene que programar, pero sí comprender las consecuencias de aprobar; la competencia de gobernanza es una responsabilidad estratégica. Las redes profesionales pueden compartir incidentes, patrones y métodos de evaluación; en tecnologías emergentes, una organización acumula pocos casos. Los repositorios anonimizados y estándares sectoriales aceleran aprendizaje; se requieren reglas para no exponer personas ni vulnerabilidades.

4.5.2. Innovación sostenible, inclusiva y centrada en la vida

La sostenibilidad integra efectos humanos, ambientales, técnicos y económicos a lo largo del ciclo; una solución que exige reemplazar dispositivos cada año puede reducir un riesgo y crear residuos o dependencia. Durabilidad, reparabilidad, consumo, materiales y logística forman parte de la compra; la evaluación compara alternativas, incluida la de no digitalizar.

La inclusión exige diseñar para diversidad y desigualdad; no todos los lugares tienen conectividad, presupuesto o especialistas. Soluciones modulares, estándares abiertos y operación local pueden ampliar acceso; la innovación que solo funciona en grandes empresas deja desprotegidos a trabajadores de pequeñas organizaciones e informalidad.

El centro es la vida, no el dato; las métricas representan dimensiones parciales y no agotan experiencia, salud o dignidad. La información ayuda a reconocer riesgo; no debe reducir a la persona a un puntaje; las decisiones de alto impacto conservan diálogo, contexto y revisión. La innovación sostenible fortalece prevención primaria; utiliza analítica para eliminar fuentes, rediseñar procesos y evaluar controles, no únicamente para adaptar conductas. La tecnología puede ayudar a visualizar lo invisible, pero la acción debe modificar condiciones; el éxito se mide por exposición y bienestar, no por cantidad de sensores.

La transición justa anticipa tareas que desaparecen, competencias y grupos afectados; la automatización de un trabajo peligroso es deseable si ofrece formación y alternativas, no si desplaza el riesgo hacia mantenimiento precario o cadenas externas. La participación permite discutir beneficios y costos antes de que se consoliden. América Latina enfrenta oportunidades y brechas de infraestructura, regulación y capacidad; la cooperación regional, los estándares interoperables y la investigación contextual pueden evitar dependencia. La obra de Rodríguez-Lindao et al. (2026) destaca retos regionales de transformación digital, privacidad y trazabilidad; aunque se centra en salud, su llamado a articular innovación, ética y contexto resulta pertinente.

Una agenda responsable combina investigación de efectividad, seguimiento de daños, gobernanza y formación; se necesitan estudios en condiciones reales, poblaciones diversas y periodos largos. También mecanismos para compartir incidentes y resultados negativos; aprender solo de productos exitosos ofrece una visión incompleta. La evaluación económica debe incluir costos evitados y cargas nuevas, sin reducir la vida a una cifra; el análisis compara mantenimiento, formación, soporte, energía, ciberseguridad y retiro. Una solución barata de adquirir puede ser costosa de gobernar; las pequeñas empresas necesitan modelos proporcionales y apoyo sectorial.

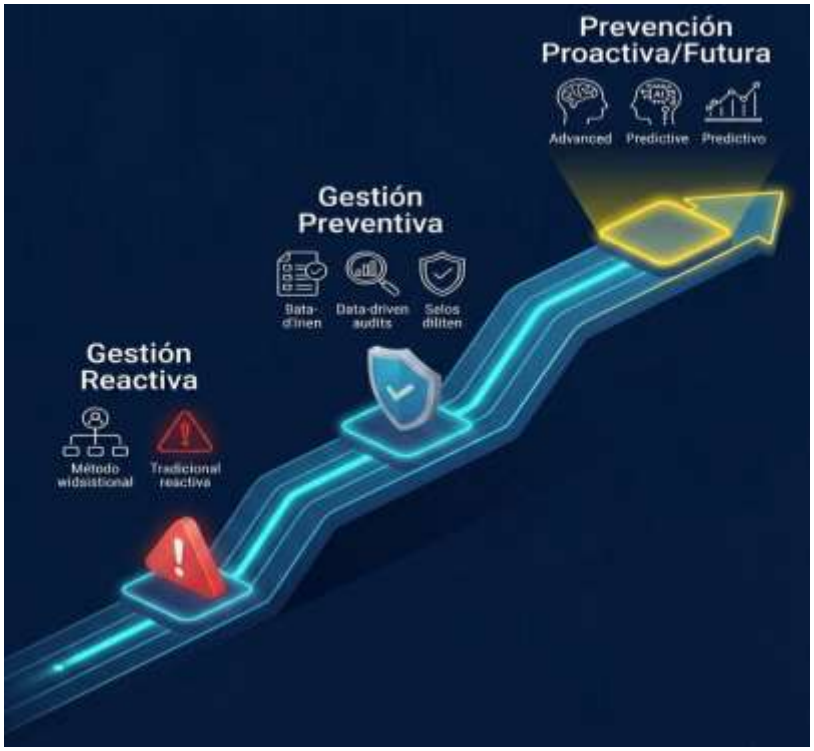
La adquisición sostenible favorece equipos reparables, contratos transparentes y proveedores que demuestran prácticas laborales responsables; también considera interoperabilidad para evitar reemplazos. La circularidad no puede comprometer seguridad: reutilizar exige verificar integridad, soporte y calibración. La inclusión se verifica mediante resultados; se analiza quién accede

a formación, quién recibe falsas alarmas y qué sedes disponen de soporte. Las brechas conducen a inversión y rediseño; declarar que una herramienta es “para todos” no constituye evidencia. La universalidad se construye con alternativas y evaluación.

La centralidad en la vida incluye el derecho a espacios no medidos; no toda actividad debe convertirse en dato. Pausas, conversaciones y autonomía cumplen funciones de salud; la organización define fronteras temporales y espaciales. La capacidad técnica de observar no crea automáticamente una finalidad legítima. El futuro seguro se construye cuando la innovación puede ser interrogada; cada sistema debe responder para qué existe, a quién beneficia, qué puede fallar, quién decide y cómo se repara. Las respuestas cambian con el contexto, pero la responsabilidad permanece; una tecnología madura no pide fe: ofrece evidencia, límites, participación y capacidad de detenerse cuando deja de proteger.

Figura 4.

Cultura de Prevención y Futuro



Referencias Bibliográficas

Ali, M. X. M., Arifin, K., Abas, A., Ahmad, M. A., Khairil, M., Cyio, M. B., Samad, M. A., Lampe, I., Mahfudz, M., & Ali, M. N. (2022). Systematic literature review on indicators use in safety management practices among utility industries. International Journal of Environmental Research and Public Health, 19(10), 6198. https://doi.org/10.3390/ijerph19106198

Amoadu, M., Ansah, E. W., & Sarfo, J. O. (2023). Influence of psychosocial safety climate on occupational health and safety: A scoping review. BMC Public Health, 23, 1344. https://doi.org/10.1186/s12889-023-16246-x

Armenteros-Cosme, P., Arias-González, M., Alonso-Rollán, S., Márquez-Sánchez, S., & Carrera, A. (2025). Advancements in artificial intelligence and machine learning for occupational risk prevention: A systematic review on predictive risk modeling and prevention strategies. Sensors, 25(17), 5419. https://doi.org/10.3390/s25175419

Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

Baines, R., Bradwell, H., Edwards, K., Stevens, S., Prime, S., Tredinnick-Rowe, J., Sibley, M., & Chatterjee, A. (2022). Meaningful patient and public involvement in digital health innovation, implementation and evaluation: A systematic review. Health Expectations, 25(4), 1232–1245. https://doi.org/10.1111/hex.13506

Cognet, B., Pernot, J.-P., Rivest, L., & Danjou, C. (2023). Systematic comparison of digital maturity assessment models. Journal of Industrial and Production Engineering, 40(7), 519–537. https://doi.org/10.1080/21681015.2023.2242340

Dodoo, J. E., Al-Samarraie, H., Alzahrani, A. I., Lonsdale, M., & Alalwan, N. (2024). Digital innovations for occupational safety: Empowering workers in hazardous environments. Workplace Health & Safety, 72(3), 84–95. https://doi.org/10.1177/21650799231215811

El-Helaly, M. (2024). Artificial intelligence and occupational health and safety, benefits and drawbacks. La Medicina del Lavoro, 115(2), e2024014. https://doi.org/10.23749/mdl.v115i2.15835

European Agency for Safety and Health at Work. (2023). Smart digital monitoring systems for occupational safety and health: Implementation at the workplace. https://healthy-workplaces.osha.europa.eu/sites/hwc/files/hwc/publication/Smart-digital-monitoring-systems-for-occupational-safety-and-health-implementation-at-the-workplace_en.pdf

European Agency for Safety and Health at Work. (2023a). Smart digital monitoring systems for occupational safety and health: Inclusion and diversity at the workplace. https://healthy-workplaces.osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-inclusion-and-diversity-workplace

European Agency for Safety and Health at Work. (2023b). Smart digital monitoring systems for occupational safety and health: Workplace resources for design, implementation and use. https://healthy-workplaces.osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-workplace-resources-design-implementation-and-use

European Agency for Safety and Health at Work. (2024). Digital technologies for worker management: Implications for safety and health. A comparative study of two automotive companies. https://healthy-workplaces.osha.europa.eu/en/publications/digital-technologies-worker-management-implications-safety-and-health-comparative-study-two-automotive-companies

European Agency for Safety and Health at Work. (2025). Principles for design and development: Smart digital systems for improving workers' safety and health. https://healthy-workplaces.osha.europa.eu/en/publications/principles-design-and-development-smart-digital-systems-improving-workers-safety-and-health

Ezerins, M. E., Ludwig, T. D., O'Neil, T., Foreman, A. M., & Açıkgöz, Y. (2022). Advancing safety analytics: A diagnostic framework for assessing system readiness within occupational safety and health. Safety Science, 146, 105569. https://doi.org/10.1016/j.ssci.2021.105569

Fisher, E., Flynn, M. A., Pratap, P., & Vietas, J. A. (2023). Occupational safety and health equity impacts of artificial intelligence: A scoping review. International Journal of Environmental Research and Public Health, 20(13), 6221. https://doi.org/10.3390/ijerph20136221

Foreman, A. M., Friedel, J. E., Ludwig, T. D., Ezerins, M. E., Açıkgöz, Y., Bergman, S. M., & Wirth, O. (2023). Establishment-level occupational safety analytics: Challenges and opportunities. International Journal of Industrial Ergonomics, 94, 103428. https://doi.org/10.1016/j.ergon.2023.103428

Citado en: capítulo 2

González-Naranjo, D. E., Román-Huera, C. K., Ponce-Regalado, D. S., Terán-Escobar, N. M., Miguez-Quincha, M. de L., Zambrano-Bravo, M. K., Mieles-Reyes, N. V., Racines-Romero, M. F., Ruiz-Sánchez, A. E., & Dominguez-Lara, O. E. (2026). Salud integral en la era digital: Bienestar físico, mental y ocupacional desde un enfoque preventivo. Oriente-Manabí Editorial. https://doi.org/10.63618/omeditorial/l8

Greer, T. W., Payne, S. C., & Thompson, R. J. (2023). Pandemic-induced telework challenges and strategies. Occupational Health Science, 7, 575–602. https://doi.org/10.1007/s41542-023-00151-1

Haas, E. J., Demich, B., & McGuire, J. (2020). Learning from workers' near-miss reports to improve organizational management. Mining, Metallurgy & Exploration, 37(3), 873–885. https://doi.org/10.1007/s42461-020-00206-9

Howard, J. (2022). Algorithms and the future of work. American Journal of Industrial Medicine, 65(12), 943–952. https://doi.org/10.1002/ajim.23429

International Labour Organization. (2021). Challenges and opportunities of teleworking in Latin America and the Caribbean. https://www.ilo.org/resource/challenges-and-opportunities-teleworking-latin-america-and-caribbean-report

International Labour Organization. (2025). Revolutionizing health and safety: The role of AI and digitalization at work. https://www.ilo.org/publications/revolutionizing-health-and-safety-role-ai-and-digitalization-work

International Organization for Standardization. (2018). ISO 45001:2018 occupational health and safety management systems—Requirements with guidance for use. https://www.iso.org/standard/63787.html

Jetha, A., Bakhtari, H., Irvin, E., Biswas, A., Smith, M. J., Mustard, C., Arrandale, V. H., Dennerlein, J. T., & Smith, P. M. (2025). Do occupational health and safety tools that utilize artificial intelligence have a measurable impact on worker injury or illness? Findings from a systematic review. Systematic Reviews, 14, 146. https://doi.org/10.1186/s13643-025-02869-1

La Torre, G., Manai, M. V., Meucci, S., Lucente, A., Picerno, A., Ammirati, S., & De Sio, S. (2026). Artificial intelligence and occupational health and safety: A systematic review. Journal of Public Health. Advance online publication. https://doi.org/10.1007/s10389-026-02738-8

Lane, M., Williams, M., & Broecke, S. (2023). The impact of AI on the workplace: Main findings from the OECD AI surveys of employers and workers (OECD Social, Employment and Migration Working Papers No. 288). OECD Publishing. https://doi.org/10.1787/ea0a0fe1-en

Mendes, D., Terradillos, E., Navas, H. V. G., Costa, O., Matias, J., & Soares, V. (2026). Wearable technologies in occupational safety and health: A systematic review and a human-centered implementation model. Applied Sciences, 16(10), 4715. https://doi.org/10.3390/app16104715

Milanez, A. (2025). Exploring win-win outcomes of algorithmic management: Lessons from a laboratory experiment on worker consultation (OECD Artificial Intelligence Papers No. 43). OECD Publishing. https://doi.org/10.1787/84b59397-en

Milanez, A., Lemmens, A., & Ruggiu, C. (2025). Algorithmic management in the workplace: New evidence from an OECD employer survey (OECD Artificial

Intelligence Papers No. 31). OECD Publishing. https://doi.org/10.1787/287c13c4-en

Oliveira, V. S., Santos, C. J. O., & Vasconcelos, B. M. (2023). Digital tools for prevention through design application: A systematic review. Work, 76(4), 1345–1356. https://doi.org/10.3233/WOR-220603

Organización Internacional del Trabajo. (2023). A call for safer and healthier working environments. https://doi.org/10.54394/HQBQ8592

Organización Internacional del Trabajo. (2025). Revolutionizing health and safety: The role of AI and digitalization at work: Global report. https://doi.org/10.54394/KNZE0733

Organización Mundial de la Salud. (2022). Directrices de la OMS sobre salud mental en el trabajo. https://www.who.int/publications/i/item/9789240053052

Organización Mundial de la Salud. (2024, 2 de septiembre). La salud mental en el trabajo. https://www.who.int/es/news-room/fact-sheets/detail/mental-health-at-work

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Rodríguez-Lindao, J. J., Castro-Barzola, L. J., Segura-Osorio, M. B., Mackliff-Jaramillo, C. G., Bravo-Moran, S. A., Rodríguez-González, D. F., Tutillo-Zambrano, D. O., Carvajal-Zuñiga, W. I., Santos-Manzaba, M. F., & Gende-Alvear, K. P. (2026). Salud digital 4.0: Aplicación de la inteligencia artificial y Big Data en la prevención, diagnóstico y gestión sanitaria. Oriente-Manabí Editorial. https://doi.org/10.63618/omeditorial/l20

Scorgie, D., Feng, Z., Paes, D., Parisi, F., Yiu, T. W., & Lovreglio, R. (2024). Virtual reality for safety training: A systematic literature review and meta-analysis. Safety Science, 171, 106372. https://doi.org/10.1016/j.ssci.2023.106372

Stefan, H., Mortimer, M., & Horan, B. (2023). Evaluating the effectiveness of virtual reality for safety-relevant training: A systematic review. Virtual Reality, 27, 2839–2869. https://doi.org/10.1007/s10055-023-00843-7

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la Unión Europea. http://data.europa.eu/eli/reg/2024/1689/oj

Vignola, E. F., Baron, S., Abreu Plasencia, E., Hussein, M., Cohen, N., & Trupin, L. (2023). Workers' health under algorithmic management: Emerging findings and urgent research questions. International Journal of Environmental Research and Public Health, 20(2), 1239. https://doi.org/10.3390/ijerph20021239

World Health Organization. (2022, December 21). Digital health not accessible by everyone equally, new study finds. https://www.who.int/europe/news/item/21-12-2022-digital-health-not-accessible-by-everyone-equally-new-study-finds

Zio, E. (2024). Digital twins in safety analysis, risk assessment and emergency management: A systematic review. Reliability Engineering & System Safety, 246, 110040. https://doi.org/10.1016/j.ress.2024.110040

Resumen

La transformación digital está modificando la gestión de la seguridad y salud en el trabajo al ampliar la capacidad de identificar peligros, integrar información y anticipar escenarios de riesgo. Este libro analiza las posibilidades de la inteligencia artificial, el Big Data, los sensores, los dispositivos portátiles, la visualización de datos, la realidad virtual y los gemelos digitales como herramientas de apoyo para una prevención más proactiva. Su planteamiento central sostiene que la eficacia de estas tecnologías no depende únicamente de su precisión o capacidad de procesamiento, sino de la calidad de los datos, su adaptación al contexto laboral y su incorporación a procesos organizacionales capaces de convertir las alertas en acciones preventivas. La obra también examina la participación de los trabajadores, la madurez digital, la usabilidad, la accesibilidad y la coordinación entre las áreas responsables de responder ante los peligros detectados. Asimismo, aborda los sesgos algorítmicos, la explicabilidad, la privacidad de los datos personales y biométricos, la ciberseguridad y la asignación de responsabilidades. Se concluye que la innovación tecnológica debe conservar una orientación humana, ética e inclusiva, fortalecer la prevención primaria y someterse a supervisión profesional. La transformación digital aporta valor cuando contribuye a reducir exposiciones, mejorar las condiciones de trabajo y proteger la salud y la dignidad de las personas.

Palabras Clave: transformación digital; seguridad y salud en el trabajo; inteligencia artificial; analítica de datos; prevención de riesgos laborales; gobernanza tecnológica.

Abstract

Digital transformation is reshaping occupational safety and health management by expanding the capacity to identify hazards, integrate information, and anticipate risk scenarios. This book examines the potential of artificial intelligence, Big Data, sensors, wearable devices, data visualization, virtual reality, and digital twins as supporting tools for more proactive prevention. Its central argument is that the effectiveness of these technologies depends not only on their accuracy or processing capacity, but also on data quality, adaptation to the workplace context, and integration into organizational processes capable of turning alerts into preventive action. The book also discusses worker participation, digital maturity, usability, accessibility, and coordination among the areas responsible for responding to identified hazards. In addition, it addresses algorithmic bias, explainability, personal and biometric data privacy, cybersecurity, and the allocation of responsibilities. It concludes that technological innovation must remain human-centered, ethical, and inclusive, strengthen primary prevention, and operate under professional oversight. Digital transformation creates meaningful value when it helps reduce occupational exposures, improve working conditions, and protect workers' health and dignity

Keywords: digital transformation; occupational safety and health; artificial intelligence; data analytics; occupational risk prevention; technology governance.

LA TECNOLOGÍA Y LOS DATOS HOY, SALVAN VIDAS MAÑANA.

La transformación digital y el análisis de datos permiten anticipar riesgos, tomar decisiones inteligentes y construir entornos de trabajo más **seguros, saludables** y **sostenibles.**

INTELIGENCIA ARTIFICIAL
Anticipa y previene riesgos laborales mediante modelos predictivos.

BIG DATA
Convierte grandes volúmenes de datos en información valiosa para la toma de decisiones.

INNOVACIÓN
Nuevas tecnologías al servicio de la seguridad, la salud y el bienestar de las personas.

GESTIÓN INTELIGENTE
Decisiones basadas en datos para entornos laborales más seguros y eficientes.

OM EDITORIAL