

EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC



JUNIO 2025

ESGinnova
Group

Simplificamos la gestión y fomentamos la **competitividad** y **sostenibilidad** de las organizaciones



Índice



ACERCA DE ESG INNOVA GROUP04

NORMAS ISO09

- ✓ Evaluación de riesgos ambientales según ISO 14001: metodologías para mejorar la gestión ambiental10
- ✓ Análisis de brechas ISO 42001: ¿debería tu compañía realizarlo?12
- ✓ Requisitos DORA: requisitos clave para el sector financiero.....14
- ✓ Cumplimiento de la norma ISO 42001: checklist para preparar la certificación..16
- ✓ Gestión del cambio en ISO 45001: pasos para una gestión eficaz de la Cláusula 8.1.318
- ✓ Cómo integrar la norma ISO 42001 con otros estándares y sistemas ISO20
- ✓ Cómo implementar ISO 14001: lista de pasos a seguir22
- ✓ ISO para inteligencia artificial: análisis de las cláusulas aplicables a sistemas de IA24
- ✓ Cuáles son los puntos de la norma ISO 9001 de 201526
- ✓ Software QMS: 5 elementos esenciales del software de gestión de calidad28
- ✓ Panorama global de las leyes de IA y cómo cumplir con la norma ISO 42001 puede ayudar30

SEGURIDAD, SALUD Y MEDIOAMBIENTE32

- ✓ Gestión de subcontratistas: claves para un entorno operativo seguro y conforme33
- ✓ Integrar seguridad y eficiencia: una estrategia operativa inteligente.....35
- ✓ Incorporación de contratistas: mejores prácticas para un proceso moderno.....37
- ✓ Cómo realizar un análisis de necesidades de capacitación en seguridad laboral39
- ✓ Software de control de contratistas: 7 beneficios clave para tu empresa en 202541
- ✓ Gestión digital de permisos de trabajo: pasos para optimizar el proceso43
- ✓ El papel del software para la gestión de seguridad y contratistas en la mejora del control de riesgos.....45
- ✓ Qué incluir en un plan de acción de emergencia en el lugar de trabajo47

Índice



✓ Cómo realizar un análisis de riesgos laborales para una evaluación eficaz.....	49
✓ Formularios de notificación de incidentes de seguridad: qué datos deben incluirse	51
GOBIERNO, RIESGO Y CUMPLIMIENTO	53
✓ Cómo afrontar los riesgos del RGPD en la Inteligencia Artificial	54
✓ Evaluación de riesgos empresariales para la toma de decisiones	56
✓ Cómo implementar programas ESG efectivos.....	58
✓ El camino hacia la Excelencia	60

ESG Innova Group

ESG Innova es un grupo de empresas con **25 años de trayectoria** en el mercado, cuyo propósito es simplificar la gestión y fomentar la competitividad y sostenibilidad de las organizaciones a nivel global. Nos implicamos en el progreso sostenible de clientes, colaboradores, socios y comunidades. En ESG Innova Group nos comprometemos con:

- 01. Salud y bienestar:** Aportando soluciones innovadoras para una gestión eficaz de la salud y seguridad de los colaboradores.
- 02. Educación de Calidad:** Contribuyendo con contenido de valor y programas formativos de primer nivel para los líderes del futuro en todo el mundo.
- 03. Igualdad de género:** Promoviendo la igualdad de oportunidades entre todos y todas los/as integrantes de la organización, independientemente de sexo, raza, ideología y religión.
- 04. Trabajo decente y crecimiento económico:** Ayudando a las organizaciones a ser más eficaces y eficientes, aportando soluciones para la gestión estratégica, táctica y operativa.
- 05. Industria, innovación e infraestructura:** Colaborando con soluciones innovadoras para el desarrollo de las organizaciones, orientándolas a ejercer un impacto positivo en criterios ESG.
- 06. Producción y consumo responsables:** Haciendo más eficiente el empleo de recursos por parte de las organizaciones, ayudándoles a mejorar en el largo plazo.
- 07. Acción por el clima:** Apoyando a nuestros clientes a reducir sus emisiones y desperdicios de recursos y extraer más rendimiento.

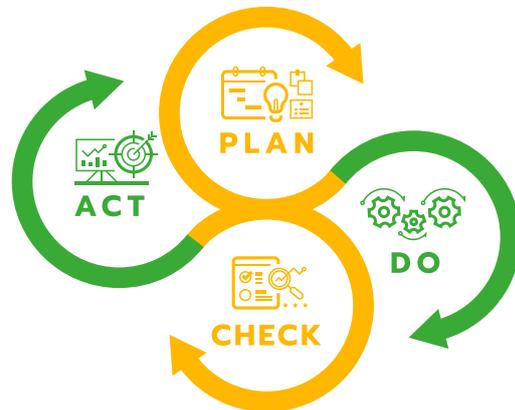
Plataforma ESG Innova

La plataforma **ESG Innova** es un entorno colaborativo en la nube en el que se desarrollan un conjunto de aplicaciones interconectadas entre sí para conformar soluciones a medida de las necesidades concretas.

❖ Motor de mejora continua

La plataforma y sus aplicaciones se basan en el ciclo de mejora continua, de aplicación en cualquier proceso.

ESGinnova
Group



❖ Plan

Facilitamos la planeación estratégica y operativa de tu organización. Te ayudamos a contar con una visión global con la que alinear personas y procesos.

❖ Do

Automatizamos los procesos de tu organización. Simplificamos la gestión para fomentar tu competitividad y también, la sostenibilidad.

❖ Check

Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ Act

Aportamos las herramientas, el conocimiento y las buenas prácticas necesarias para que su organización recorra el camino de la mejora continua.

Unidades de negocio

ESG Innova es un grupo internacional de empresas, líder en **transformación digital para organizaciones de ámbito público y privado** a nivel mundial. Se trata de una entidad que se preocupa en desarrollar soluciones tecnológicas que aporten valor a organizaciones, inversores, y organismos públicos.



ESG Innova cuenta con productos que dan cobertura a diferentes marcos de trabajo en materia de **gobierno corporativo, gestión integral de riesgos, cumplimiento normativo y HSE (Health, Safety and Environment)** lo que permite que estos se adapten a los nuevos retos del mercado y a las necesidades de las organizaciones.

Estas líneas de solución las trasladamos al día a día de las organizaciones con el apoyo de la **presencia local, con oficinas, partners y colaboradores a lo largo de todo el mundo.**

Unidades de negocio

Estas líneas de solución las trasladamos al día a día de las organizaciones con el apoyo de la **presencia local, con diferentes oficinas, partners y colaboradores a lo largo de todo el mundo.**

ISOTools

Transformación Digital para los Sistemas de Gestión Normalizados y Modelos de Gestión y Excelencia.

HSETools

Transformación Digital para los Sistemas de Salud, Seguridad y Medioambiente.

GRCTools

Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento.

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo



Menos de tiempo de resolución de una acción correctiva



Menos de tiempo de preparación de las reuniones de gestión



Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes



Menos de intercambios de documentación física entre sedes y dptos.



Menos de costes indirectos derivados de la gestión documental



La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento



Más de optimización en el sistema de gestión tras la etapa de consultoría



Más capacidad de resolución de problemas del sistema de gestión

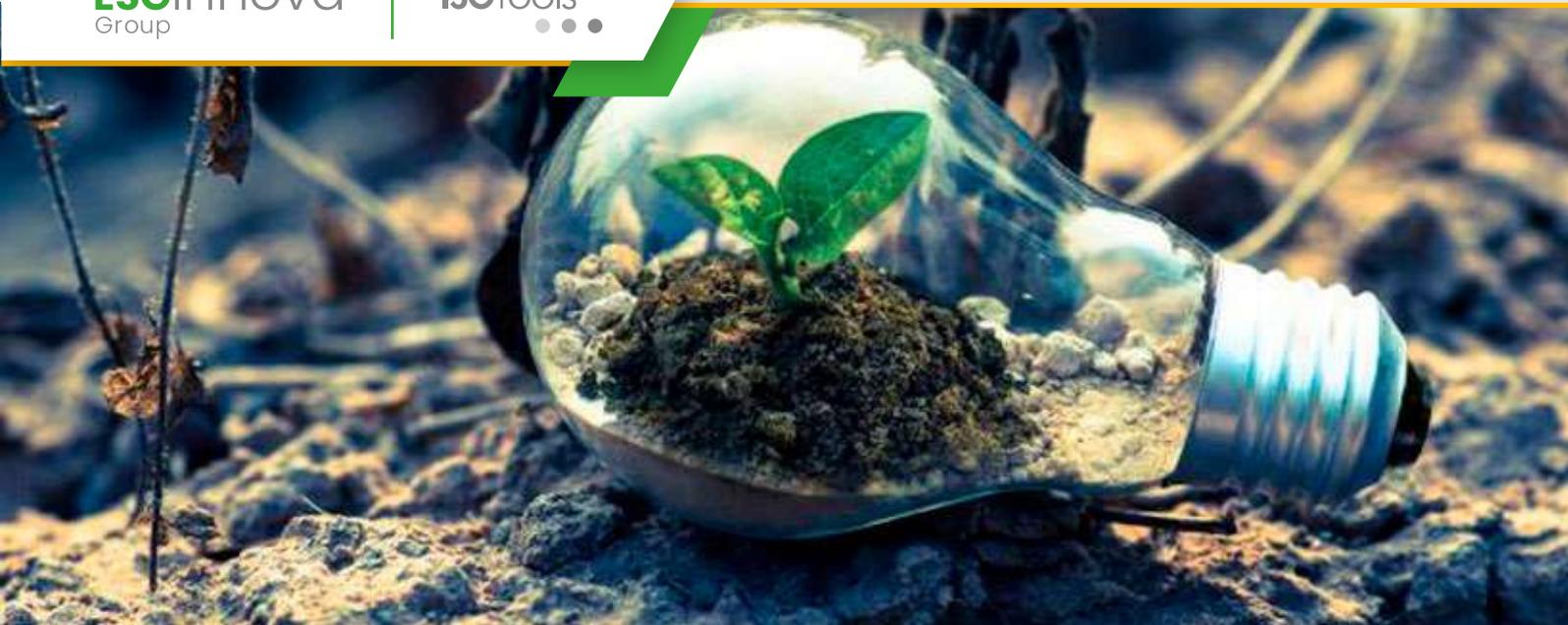


Más de trabajadores implicados en la gestión del sistema

ISOTools



Transformación Digital
para la gestión
de **Sistemas**
Normalizados ISO



Evaluación de riesgos ambientales según ISO 14001: metodologías para mejorar la gestión ambiental

La **evaluación de riesgos ambientales** es una práctica obligatoria, estratégica y de alto valor para la gestión ambiental según la **norma ISO 14001**. Existen múltiples metodologías para realizar esta evaluación y su elección dependerá del contexto en el que opera cada organización y de su sector.

El propósito de esta guía es ofrecer una definición precisa del concepto de evaluación de riesgos ambientales, explicar sus objetivos y presentar **las principales metodologías que existen para realizarla**.

¿Cuál es el objetivo de la evaluación de riesgos ambientales?

La evaluación de riesgos ambientales tiene como finalidad identificar, calificar y priorizar los riesgos asociados con los aspectos ambientales de la organización. Para realizar esta tarea, **se consideran todos los riesgos**, sin tener en cuenta aún su gravedad o su probabilidad de ocurrencia.

Con una lista completa de posibles eventualidades, la evaluación de riesgos ambientales avanza con la **categorización y priorización de las amenazas**, de acuerdo con su impacto y su probabilidad de ocurrencia.

La **gestión de riesgos ambientales** termina el trabajo determinando las **acciones de tratamiento apropiadas para cada riesgo**. Algunos podrán ser eliminados, otros mitigados en su impacto, otros trasladados o compartidos y, los que restan, serán aceptados.

¿Qué establece ISO 14001 sobre la evaluación de riesgos ambientales?

La norma ISO 14001 define la evaluación de riesgos ambientales como un proceso sistemático para identificar aspectos ambientales, establecer su importancia y definir las acciones de tratamiento adecuadas. Para hacerlo, **ISO 14001 considera que la evaluación necesita incorporar cinco elementos clave:**

- **Aspectos ambientales:** elementos, condiciones, circunstancias, actividades, procesos, productos o servicios que pueden interactuar con el medio ambiente, con efectos positivos o negativos.



Análisis de brechas ISO 42001: ¿debería tu compañía realizarlo?

El **análisis de brechas ISO 42001** debería ser el primer paso en el proceso de implementación de un sistema de gestión de Inteligencia Artificial. A pesar de su relevancia estratégica, aún hay profesionales que lo consideran opcional e incluso innecesario, subestimando sus beneficios reales.

El análisis de brechas ISO 42001, también denominado evaluación de preparación, permite determinar el estado del sistema frente a los requisitos del estándar internacional de Inteligencia Artificial. Es decir, **identifica lo que ya se ha implementado y lo que falta por desarrollar** para cumplir con la norma. No realizar el análisis de brechas ISO 42001 expone a la organización a riesgos innecesarios: operaciones de retrabajo, duplicación de tareas y pérdida de eficiencia.

¿Qué es ISO 42001?

ISO 42001 es el primer estándar internacional específicamente **diseñado para abordar los riesgos derivados del desarrollo y uso de sistemas de IA**. Publicado en diciembre de 2023, adopta la estructura de Alto Nivel que caracteriza a estándares tan reconocidos como **ISO 9001**, ISO 45001 o ISO 14001.

Además de sus **siete capítulos de requisitos**, ISO 42001 incluye anexos con controles específicos y directrices para su aplicación. Entre los **posibles riesgos de seguridad de la IA** que busca mitigar destacan los sesgos, la discriminación, la autodeterminación de los sistemas, la pérdida de privacidad, la amenazas a los derechos humanos o problemas relacionados con la propiedad intelectual, entre otros muchos.

ISO 42001 se convierte así en la herramienta más efectiva para demostrar a clientes, consumidores, inversores, reguladores y a la sociedad que la empresa **hace un uso transparente, seguro, ético, inclusivo y equitativo de la nueva tecnología**.

¿Cómo iniciar el trabajo de implementación de ISO 42001?

La **implementación de ISO 42001** es una tarea desafiante. La primera pregunta que se hacen los impulsores del proyecto es por dónde comenzar. En cuanto a esto, es evidente que **la recomendación natural es empezar con el análisis de brechas**.

Este se enfoca en aspectos esenciales para la gestión de riesgos de IA, como la equidad y la inclusión, la accesibilidad, la seguridad de los datos o la ética.



Requisitos DORA: requisitos clave para el sector financiero

La gestión de riesgos digitales se ha convertido en una prioridad estratégica para las organizaciones del sector financiero. En este contexto, los **requisitos DORA** (Digital Operational Resilience Act) marcan un antes y un después en la regulación europea y también impactan en la implementación de estándares como **ISO 27001**.

El Reglamento, plenamente aplicable desde enero de 2025, **establece un marco legal homogéneo para garantizar la resiliencia operativa digital** en el ecosistema financiero. Pero, ¿cuáles son exactamente los requisitos DORA y cómo impactan en los sistemas de gestión normalizados? Lo analizamos a continuación.

¿Qué es DORA y por qué es relevante para el sector financiero?

La **Regulación DORA** (Reglamento 2022/2554) fue aprobado por el Parlamento Europeo en 2022 como parte de un paquete legislativo para reforzar la infraestructura digital del sistema financiero. Su objetivo principal es **garantizar que las entidades financieras de**

la UE puedan resistir, responder y recuperarse de incidentes relacionados con las TIC, asegurando la continuidad del negocio y la confianza del mercado.

Frente a otras normativas centradas en la seguridad de la información o en la protección de datos, DORA da un paso más: **aborda de forma integral la gestión de riesgos TIC**, desde la gobernanza interna hasta las pruebas de resiliencia y la supervisión de proveedores externos.

¿A qué organizaciones afecta la regulación DORA?

Los requisitos DORA **se aplican a una amplia gama de entidades financieras**. Entre ellas, se incluyen las siguientes:

- Bancos.
- Aseguradoras y reaseguradoras.
- Empresas de inversión.
- Entidades de pago y dinero electrónico.
- Sociedades de gestión de activos.
- Proveedores de servicios de criptoactivos.

También deben **cumplir con la normativa DORA proveedores críticos de servicios TIC**, como es el caso de empresas de servicios en la nube, proveedores de software o servicios de ciberseguridad.



Cumplimiento de la norma ISO 42001: checklist para preparar la certificación

La IA es ya un pilar estratégico para muchas organizaciones, transformando procesos, productos y servicios. Sin embargo, su adopción también plantea desafíos éticos, de seguridad y de gobernanza. Para afrontarlos, el **cumplimiento de la norma ISO 42001** es esencial.

El estándar internacional proporciona **un marco sólido para implementar sistemas de gestión de inteligencia artificial** que aseguran un uso responsable, seguro y ético de esta tecnología. El proceso es complejo, de ahí la importancia de contar con una guía detallada para preparar la certificación en base al cumplimiento de la norma ISO 42001.

¿Cuál es la relevancia de la norma ISO 42001?

ISO 42001 proporciona directrices para establecer, implementar, mantener y mejorar continuamente un **sistema de gestión de**

inteligencia artificial. Su adopción ofrece a las organizaciones ventajas interesantes:

- Demostrar compromiso con un **uso responsable de tecnologías de IA**, garantizando que los sistemas desarrollados **respetan los principios fundamentales** de derechos humanos, privacidad y equidad.
- **Gestionar riesgos** asociados a la implementación de sistemas de IA, incluyendo los riesgos tecnológicos, operativos, reputacionales y legales.
- **Cumplir con requisitos legales** y regulatorios en constante evolución, como la **Ley de Inteligencia Artificial de la UE** o normativas nacionales específicas.
- **Fomentar la confianza** entre clientes, socios y otras partes interesadas, al adoptar un estándar reconocido internacionalmente.

La implementación y el cumplimiento de la norma ISO 42001 se convierte así en mucho más que una herramienta de gestión. Es una **declaración de principios para que el uso de la inteligencia artificial sea seguro** y dirigido por procesos claros y auditables.

Cumplimiento de la norma ISO 42001 paso a paso

Preparar la **certificación de la norma ISO 42001** requiere de **tiempo, recursos y profesionales altamente cualificados**, además de herramientas tecnológicas que agilicen todo el proceso.



Gestión del cambio en ISO 45001: pasos para una gestión eficaz de la Cláusula 8.1.3

Los cambios son inevitables en cualquier organización: se desarrollan nuevas tecnologías, hay reorganizaciones internas o se producen ajustes legislativos. En este contexto, la **gestión del cambio en ISO 45001** se convierte en una herramienta clave para garantizar que estos cambios no comprometan la seguridad ni la salud de los trabajadores.

ISO 45001 es una norma reconocida a nivel internacional para sistemas de gestión de la seguridad y salud en el trabajo. Su Cláusula 8.1.3 exige la implantación de procesos estructurados para **anticipar, evaluar y controlar los riesgos** derivados de cualquier modificación significativa en el entorno laboral. Para llevar a cabo una correcta gestión del cambio en ISO 45001 **es necesario un conocimiento profundo tanto de la norma como del proceso**. A continuación, se detallan las etapas clave, resaltando sus beneficios organizacionales y el papel esencial de la tecnología como aliada estratégica.

¿Qué exige ISO 45001 sobre la gestión del cambio?

La norma internacional ISO 45001 establece en su Cláusula 8.1.3 la **necesidad de implementar un proceso para gestionar los cambios** que puedan afectar al **Sistema de Gestión de Seguridad y Salud en el Trabajo** (SGSST). Esto incluye cambios en:

- Productos, servicios o procesos.
- Organización interna o ubicación.
- Equipos, personal y recursos materiales.
- Requisitos legales o del contexto.
- Condiciones laborales.
- Información sobre riesgos y oportunidades.

La norma exige **considerar tanto cambios planificados (temporales o permanentes) como no planificados** y documentar las consecuencias para tomar acciones correctivas oportunas.

El objetivo es anticipar, evaluar y controlar los riesgos antes de que se implementen los cambios para minimizar el riesgo de incidentes y preservar la salud de los trabajadores



Cómo integrar la norma ISO 42001 con otros estándares y sistemas ISO

La gestión de la inteligencia artificial en las organizaciones modernas requiere un enfoque sistemático que trascienda las fronteras de los sistemas de gestión aislados. En este contexto, **integrar la norma ISO 42001** con otros estándares ISO se posiciona como una estrategia clave para construir un ecosistema de gestión coherente y eficaz.

Integrar la norma ISO 42001 no solo optimiza recursos y procesos. También **fortalece la capacidad de las organizaciones para abordar los desafíos complejos** que plantea la implementación responsable y ética de sistemas de inteligencia artificial en el entorno empresarial.

¿Qué es la norma ISO 42001 y por qué es relevante su integración?

ISO 42001 es el primer **estándar para sistemas de gestión de inteligencia artificial** de carácter internacional. Este marco normativo **establece requisitos para la implementación, mantenimiento y mejora continua** de sistemas en organizaciones que desarrollan, implementan o utilizan productos y servicios basados en la IA.

La relevancia de esta norma radica en su **capacidad para abordar los riesgos asociados a la inteligencia artificial**, incluyendo consideraciones éticas y de transparencia, rendición de cuentas, mitigación de sesgos, seguridad y privacidad. A diferencia de otros estándares de IA, ISO 42001 adopta el enfoque de sistema de gestión basado en el método PDCA de mejora continua, lo que facilita su integración natural con otros estándares ISO.

Integrar la norma ISO 42001 con otros sistemas de gestión normalizados permite a las organizaciones **desarrollar un enfoque holístico y coherente hacia la gestión de riesgos, calidad y cumplimiento regulatorio**. Esta sinergia resulta especialmente valiosa en un entorno donde la IA interacciona con aspectos operacionales y estratégicos de muchas organizaciones.

Beneficios de integrar la norma ISO 42001 con otros estándares de gestión

Integrar la norma ISO 42001 ofrece ventajas significativas a las organizaciones que apuestan por integrar estándares en lugar de aplicarlos por separado.



ISO

Cómo implementar ISO 14001: lista de pasos a seguir

Saber **cómo implementar ISO 14001** es el primer paso para que una organización sea capaz de gestionar sus aspectos ambientales de forma eficaz. El estándar internacional de sistemas de gestión ambiental no solo ayuda a reducir impactos negativos en el entorno, sino que también impulsa el cumplimiento legal, la eficiencia operativa y la competitividad.

A la hora de abordar el proceso de cómo implementar ISO 14001 es necesario tener presente que **requiere de visión estratégica y, sobre todo, de una hoja de ruta** claramente estructurada. Esta debe ser realista y estar alineada con los requisitos de la norma y las características de la organización.

Elementos clave previos al proceso de implementación

- Antes de iniciar la implementación de ISO 14001, es muy importante realizar un análisis de brechas. Es lo que permitirá **evaluar el punto de partida del SGA**. En esta fase previa es fundamental:

- **Contar con una política ambiental sólida** y avalada por la Alta Dirección.
- Tener un registro actualizado de los requisitos legales.
- Elaborar un mapa de aspectos e impactos ambientales significativos.
- **Definir los objetivos**, metas y programas de mejora.
- **Nombrar a un responsable** del SGA con autoridad dentro del equipo directivo.

Cómo implementar ISO 14001 paso a paso

Con estos primeros pasos ya dados, se podrá comenzar el proceso de implementación de la norma. **Comprender cómo implementar ISO 14001 paso a paso permite evitar errores** y maximizar resultados.

1. Compromiso de la dirección

El **papel de la Alta Dirección** y su compromiso son esenciales por dos motivos: el primero, para contar con los recursos humanos, técnicos y financieros necesarios; el segundo, para posicionar al SGA como prioridad estratégica. En este último aspecto, hay que tener en cuenta que ISO 14001 señala que **el liderazgo es requisito para que el sistema de gestión pueda sostenerse**.

Cómo implementar ISO 14001 con éxito requiere asegurar este liderazgo desde el inicio. El apoyo de la Alta Dirección se puede alcanzar **presentando cifras de retorno de la inversión y ventajas competitivas**.



ISO para inteligencia artificial: análisis de las cláusulas aplicables a sistemas de IA

La creciente adopción de sistemas basados en inteligencia artificial ha impulsado la necesidad de establecer marcos normativos que garanticen un uso responsable, ético y seguro de esta tecnología. En este contexto, la **norma ISO para inteligencia artificial, ISO 42001**, es el primer estándar internacional específicamente diseñado para implementar sistemas de gestión de IA en organizaciones que desarrollan, utilizan o proporcionan soluciones basadas en inteligencia artificial.

Más allá de establecer buenas prácticas, el estándar introduce un modelo auditable que permite a las organizaciones demostrar su compromiso con la **gobernanza de la inteligencia artificial**. ISO 42001 **integra criterios éticos, de transparencia, trazabilidad** y gestión del ciclo de vida de los sistemas de IA.

¿Cuál es la estructura de la norma ISO para inteligencia artificial?

ISO 42001 **adopta una estructura de alto nivel**, común en otras normas de sistemas de gestión como **ISO 27001** o ISO 9001. Esta estructura permite integrar fácilmente el sistema de gestión de IA con otros ya existentes.

Las cláusulas 1 a 3 de la norma ISO para inteligencia artificial se centran en el contexto y proporcionan términos y definiciones. Las cláusulas 4 a 10, por su parte, se refieren a los requisitos fundamentales y auditables de un SGIA. A estas cláusulas hay que sumar los controles del Anexo A, que se deben evaluar y aplicar según el análisis de riesgos propio de cada organización.

Cláusula 4: Contexto de la organización

Comprender el entorno interno y externo de la organización es esencial para definir el alcance del sistema de gestión de la IA. ISO 42001 **exige identificar los factores que afectan al desarrollo y uso de esta tecnología**, desde aspectos relacionados con la normativa a preocupaciones éticas o **riesgos asociados a la IA**.

La organización debe también analizar las expectativas de partes interesadas y establecer límites claros para su sistema de gestión de IA. Este análisis contextual **condiciona el diseño de políticas, la asignación de recursos y el enfoque de tratamiento de riesgos**.

Cláusula 5: Liderazgo

El liderazgo efectivo es motor del cumplimiento, por ello, **corresponde a la alta dirección asumir la responsabilidad**.



Cuáles son los puntos de la norma ISO 9001 de 2015

Cuando una organización decide implementar un sistema de gestión de la calidad, una de las primeras preguntas que se plantea es: **¿por dónde empiezo?** La respuesta más directa y eficaz pasa por conocer en profundidad la **ISO 9001 de 2015**, la norma internacional que establece los requisitos para garantizar la calidad en productos y servicios, con una orientación clara hacia la mejora continua y la satisfacción del cliente.

En este artículo desglosamos los puntos clave que estructuran esta norma, su lógica interna y su valor práctico para organizaciones de todos los sectores. También veremos cómo herramientas digitales como el **Software ISO 9001 de ISOTools** facilitan su aplicación y seguimiento, optimizando cada uno de sus apartados.

ISO 9001 de 2015: Una norma centrada en el valor

La versión 2015 de la **ISO 9001** marcó un antes y un después respecto a sus ediciones anteriores. Se introdujeron conceptos modernos como el **pensamiento basado en riesgos**, el enfoque a

procesos fortalecido y una integración más natural con otras normas ISO gracias a la estructura de alto nivel (HLS, por sus siglas en inglés).

El objetivo de esta norma es que las organizaciones documenten procesos, y pongan el foco en **generar valor real**, entregando productos y servicios que cumplan con los requisitos del cliente, optimizando sus recursos y asegurando la sostenibilidad de su operación.

Cuando una organización decide implementar un sistema de gestión de la calidad, una de las primeras preguntas que se plantea es: **¿por dónde empiezo?** La respuesta más directa y eficaz pasa por conocer en profundidad la **ISO 9001 de 2015**, la norma internacional que establece los requisitos para garantizar la calidad en productos y servicios, con una orientación clara hacia la mejora continua y la satisfacción del cliente.

En este artículo desglosamos los puntos clave que estructuran esta norma, su lógica interna y su valor práctico para organizaciones de todos los sectores. También veremos cómo herramientas digitales como el **Software ISO 9001 de ISOTools** facilitan su aplicación y seguimiento, optimizando cada uno de sus apartados.

ISO 9001 de 2015: Una norma centrada en el valor

La versión 2015 de la **ISO 9001** marcó un antes y un después respecto a sus ediciones anteriores. Se introdujeron conceptos modernos como el **pensamiento basado en riesgos**, el enfoque a procesos fortalecido y una integración más natural con otras normas ISO gracias a la estructura de alto nivel (HLS, por sus siglas en inglés).



Software QMS: 5 elementos esenciales del software de gestión de calidad

La implantación de un sistema de gestión de calidad conforme con la norma **ISO 9001** requiere herramientas capaces de sostener, coordinar y optimizar todos los procesos implicados. En este contexto, contar con un **software QMS** (Quality Management System) no solo facilita el cumplimiento normativo, sino que se convierte en aliado estratégico para alcanzar la mejora continua.

Frente a la creciente complejidad de los entornos empresariales y regulatorios, un software QMS que integre los requisitos de ISO 9001 ofrece a las organizaciones **una plataforma robusta y ágil para garantizar la calidad y minimizar los riesgos**. Esta herramienta tecnológica no sustituye el sistema, sino que lo hace operativo, medible y escalable.

Elementos clave en un software QMS

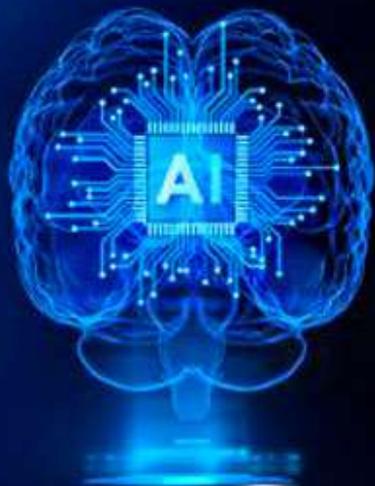
Elegir un **software de calidad** es una decisión compleja. Previamente es necesario definir los requisitos específicos del sistema de la organización y **valorar aspectos esenciales y funcionalidades básicas**. Los que se mencionan a continuación son especialmente relevantes.

1. Objetivos de calidad bien definidos

Establecer objetivos de calidad claros y medibles es uno de los **requisitos de la norma ISO 9001** y, al mismo tiempo, es motor de mejora dentro de cualquier organización. Estos objetivos **deben estar alineados con la política de calidad, ser coherentes con la estrategia global de la empresa** y servir como punto de referencia para evaluar su desempeño.

Estos objetivos **deben cumplir criterios SMART** (específicos, medibles, alcanzables, significativos y con plazo definido). Por ejemplo, un objetivo como puede ser reducir el índice de devoluciones de un producto del 4 % al 2 % en seis meses requiere datos actuales, históricos y en tiempo real para analizar la evolución, detectar causas raíz y aplicar acciones correctivas.

Un software QMS debe ofrecer funcionalidades que permitan configurar estos objetivos, asociarlos a **indicadores clave de calidad**, asignar responsables y plazos y hacer un seguimiento visual de su avance. También debe generar alertas automáticas en caso de desviaciones y facilitar informes para la revisión por parte de la dirección.



Panorama global de las leyes de IA y cómo cumplir con la norma ISO 42001 puede ayudar

La creciente adopción de sistemas de inteligencia artificial está generando oportunidades sin precedentes. Sin embargo, también plantea riesgos legales, éticos y sociales que exigen una regulación sólida. En este contexto, las **leyes de IA** se han convertido en eje básico del cumplimiento normativo. **ISO 42001** ofrece a las organizaciones un marco para gestionarlas de forma responsable y alineada con los estándares globales.

Comprender este **entorno normativo en rápida evolución** es esencial para diseñar, implementar y supervisar sistemas de IA con garantías. Desde marcos regulatorios estrictos hasta enfoques más flexibles, los países están definiendo cómo regular el desarrollo y uso de la inteligencia artificial.

Para las organizaciones, **adoptar un sistema de gestión basado en ISO 42001 significa anticiparse a los requisitos legales**, minimizar **riesgos de la IA** y consolidar una cultura de innovación ética y trazable.

Principales leyes de IA en el mundo

El término leyes de IA no se refiere a una única norma, sino a **un conjunto diverso de marcos regulatorios que evolucionan rápidamente**. A continuación, se desglosan los más relevantes a nivel global:

América del Norte

Estados Unidos mantiene un enfoque descentralizado respecto a las leyes de IA. La derogación de la Orden Ejecutiva Federal de 2023 deja en manos de los estados la responsabilidad regulatoria. Colorado se posiciona a la vanguardia con la Colorado AI Act, en vigor desde mayo de 2024, que impone obligaciones específicas a los desarrolladores y operadores de sistemas de alto riesgo. Otros estados como California y Virginia han desarrollado normativas centradas en la privacidad algorítmica y la equidad.

Por su parte, **Canadá avanza con el proyecto de Ley de Inteligencia Artificial y Datos (AIDA)**, que establece sanciones ante el uso negligente de sistemas de IA y contempla la creación de un Comisionado de IA para asegurar la vigilancia regulatoria.

Unión Europea

La **Ley de Inteligencia Artificial de la UE**, que entró en vigor en agosto de 2024, es el primer marco legal integral del mundo para regular esta tecnología.

HSETools



Transformación Digital
para la gestión
de **Seguridad, Salud
y Medioambiente**



Gestión de subcontratistas: claves para un entorno operativo seguro y conforme

La **gestión de subcontratistas** es tan importante como la que se realiza para garantizar la seguridad y una excelente relación con la fuerza laboral externa representada por los **contratistas**. Ignorar esta realidad implica exponer a la organización a riesgos evitables que afectan a la seguridad, al cumplimiento normativo y al rendimiento operativo. Las organizaciones han desarrollado **una alta dependencia de contratistas** para ejecutar proyectos dentro y fuera de sus instalaciones. Las razones son varias: costes, conocimiento y habilidad, necesidad de ubicar trabajadores en áreas remotas, etc. Esa creciente dependencia añade un eslabón en la cadena de suministro: los subcontratistas. Por ello, la gestión de subcontratistas **es una responsabilidad que se suma a las ya existentes para los equipos de SST**. Sin embargo, hay que superar un desafío: la idea de que la gestión de subcontratistas es una responsabilidad exclusiva del contratista. Es una premisa que puede significar problemas para los mismos subcontratistas, para los contratistas y para la organización.

Consecuencias de no asumir la gestión de subcontratistas

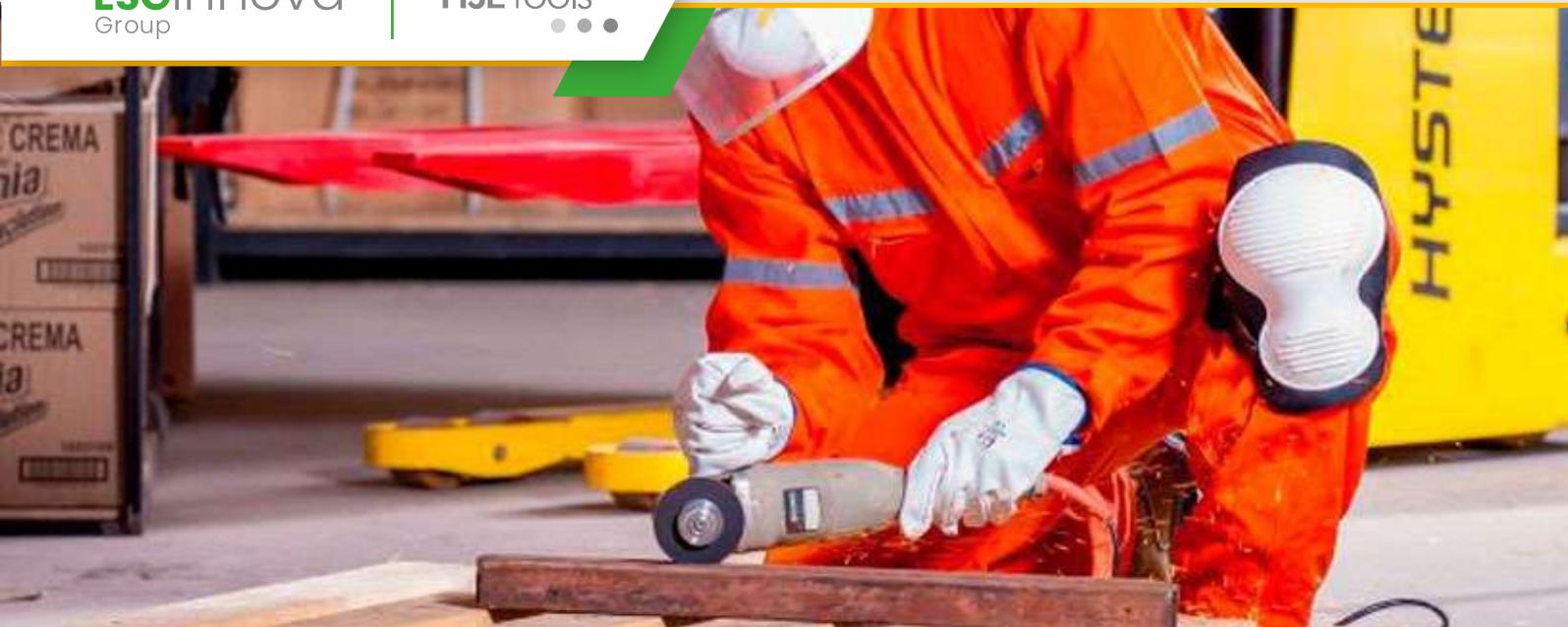
Entre empresa, contratistas y subcontratistas se crea una **cadena de suministro**, pero también una cadena de dependencia y de autoridad. Así, parece coherente que la **responsabilidad HSE** y, más en concreto, la gestión de subcontratistas, corresponda a sus superiores jerárquicos inmediatos. No obstante, **es probable que el contratista no cuente con la estructura** de gobernanza, tecnológica y financiera adecuada para garantizar la seguridad y el bienestar de sus trabajadores. Las **consecuencias de una mala gestión**, la ausencia de una gestión de subcontratistas sistemática, técnica y estructurada, puede ser demoledora. Se trata de problemas que de una forma u otra afectarán con mayor intensidad a la organización. **Los riesgos se pueden agrupar en tres categorías:**

1. Riesgos de seguridad

El riesgo de accidentes aumenta por el **desconocimiento del entorno de trabajo, de los protocolos internos y de las normas de seguridad**. El subcontratista encuentra en su empleador, el contratista, el conducto para expresar cualquier preocupación sobre seguridad laboral, uso de **elementos de protección personal** u otros temas relacionados. Sin embargo, los contratistas no siempre cuentan con recursos apropiados para resolver esas solicitudes.

2. Riesgos de cumplimiento

La ausencia de gestión de subcontratistas puede generar una zona gris en la que nadie asuma responsabilidades impuestas por la ley, directivas o reglamentos que aplican a una determinada industria. **Este incumplimiento genera sanciones**, multas, cierre de operaciones y pérdida de licencias.



Integrar seguridad y eficiencia: una estrategia operativa inteligente

Integrar **seguridad y eficiencia** en un mismo entorno de trabajo, de forma natural y sin que uno de los dos elementos reste valor al otro en los **programas HSE**, es uno de los mayores desafíos a los que se enfrentan los equipos de seguridad y salud en el trabajo.

Elegir entre seguridad y eficiencia es también un dilema en las juntas directivas de las organizaciones. Es evidente que a todos, incluidos los líderes de SST, les **interesa que la empresa alcance sus objetivos comerciales**. También es cierto que la **gestión de seguridad y salud en el trabajo** implica una inversión significativa. **Ese coste puede percibirse como un factor que afecta la capacidad financiera** de la empresa para impulsar proyectos de crecimiento. Además, los ejecutivos del área comercial o de producción y la Alta Dirección pueden pensar que algunas normas de seguridad ralentizan la productividad y limitan la capacidad para lograr objetivos comerciales. Sin embargo, esta visión no tiene en cuenta un aspecto esencial: **espacios de trabajo seguros, confortables y**

saludables, impulsan la productividad. Los trabajadores que se sienten seguros y valorados rinden más y mejor. Por eso, la pregunta no es si priorizar seguridad o eficiencia, sino cómo integrarlas de forma inteligente.

Cómo integrar seguridad y eficiencia dentro de una estrategia operativa eficaz

Integrar seguridad y eficiencia en una organización requiere desplegar estrategias inteligentes. El objetivo prioritario será **demostrar que la inversión en seguridad no solo protege, sino que también optimiza recursos**, mejora la calidad y reduce costes. Las siguientes **seis estrategias han demostrado efectividad** en muchas empresas, en el propósito de integrar seguridad y eficiencia:

1. Capacitar a los empleados en seguridad y prevención

El objetivo de los **programas de seguridad y salud en el trabajo** es **enseñar a los empleados a realizar sus tareas diarias implementando procedimientos seguros**, utilizando equipos de protección personal adecuados e inspeccionando el lugar de trabajo de forma constante para advertir la aparición de nuevos riesgos. Impartir formación y capacitación tiene un coste que aumenta con el valor de las horas que destinan los trabajadores a recibir los programas. Sin embargo, los empleados no solo aprenden a hacer las cosas con seguridad, también a hacerlas de forma eficiente y correcta. **El primer resultado tangible es un incremento de los niveles de calidad.** Existe además un beneficio financiero en la capacitación: la **eliminación del coste de atención médica, de reentrenamiento** cuando es preciso ubicar un trabajador como reemplazo de emergencia y de sanciones regulatorias y legales. Esto, sin mencionar el coste de la ausencia del trabajador lesionado.



Incorporación de contratistas: mejores prácticas para un proceso moderno

La **incorporación de contratistas** es una fase crítica en la gestión operativa y de cumplimiento normativo de muchas organizaciones. Bien para cubrir necesidades puntuales, bien para ejecutar proyectos especializados o reforzar equipos en momentos críticos, el trabajo con fuerza laboral externa es esencial en infinidad de sectores productivos. Sin embargo, su integración efectiva sigue siendo un desafío dentro de la **gestión de contratistas**.

En un contexto donde la presión por el cumplimiento legal y normativo se combina con la necesidad de actuar con rapidez y sin errores, **la gestión manual del proceso de incorporación de contratistas no es viable**. Formularios en papel, cadenas de correos, verificaciones dispersas y formaciones descoordinadas pueden significar retrasos, **brechas de cumplimiento** o de seguridad y sanciones regulatorias. Por ello, **modernizar el proceso de incorporación de contratistas debe ser una prioridad** para aquellas organizaciones que necesitan ser más competitivas. A

continuación, se analizan los principales puntos críticos y las mejores prácticas para una correcta incorporación de contratistas desde el punto de vista de la automatización, el cumplimiento y la eficiencia operativa.

Cuáles son los puntos críticos en la incorporación de contratistas

Los enfoques tradicionales en la contratación de fuerza laboral externa presentan deficiencias que pueden significar retrasos, incumplimientos normativos e incluso pérdidas económicas. **Esos desafíos se concentran, fundamentalmente, en tres cuestiones:**

Procesos manuales propensos al error

Recepción de documentos por correo electrónico, comprobaciones con hojas de cálculo, capacitaciones presenciales sin trazabilidad ni registros digitalizados no solo ralentizan el proceso, sino que **umentan el riesgo de errores humanos, pérdida de información e incluso incidentes de seguridad.**

Dificultad para garantizar cumplimiento

La normativa en materia de seguridad y salud laboral, como **ISO 45001**, exige cumplir con unos estrictos criterios respecto a contratistas y subcontratistas. Organizaciones que no controlan estos aspectos pueden incurrir en incumplimientos que **afectarán a su reputación y pueden derivar en sanciones económicas.** Además de todo ello, es esencial tener en cuenta que los requisitos pueden variar según el país o la actividad de la organización.



Cómo realizar un análisis de necesidades de capacitación en seguridad laboral

En un entorno empresarial cada vez más regulado y competitivo, garantizar la seguridad y salud de los trabajadores no es solo una obligación legal, sino una estrategia esencial para la maximizar la eficiencia operativa. Realizar un **análisis de necesidades de capacitación** en seguridad laboral dentro de los **programas HSE** es el primer paso en ese camino.

El análisis de necesidades de capacitación permite a las organizaciones **identificar brechas en habilidades y conocimientos**. Esa evaluación es la que hará posible alinear la formación con los objetivos empresariales, la evolución normativa y los nuevos retos operativos.

¿Qué es un análisis de necesidades de capacitación?

Un análisis de necesidades de capacitación es un proceso sistemático que **identifica las discrepancias** que existen entre las competencias actuales de los empleados y las requeridas para desempeñar sus

funciones de manera segura y eficiente. Este análisis no solo detecta carencias, sino que también **orienta el desarrollo de programas de formación** específicos que cumplen con las regulaciones y ayudan a **maximizar el rendimiento HSE**.

Tipos de análisis de necesidades de capacitación

Existen diferentes enfoques a la hora de analizar y evaluar las necesidades de capacitación en seguridad laboral. Estos **pueden combinarse según el contexto** y los objetivos de la organización:

Análisis organizacional

Evalúa las metas de la empresa, los indicadores de desempeño y los riesgos corporativos para determinar en qué aspectos se requiere capacitación. Este tipo de análisis es útil para integrar la seguridad en la estrategia general de la empresa.

Análisis de tareas

Identifica competencias específicas necesarias para realizar tareas críticas con seguridad. **Incluye observaciones directas y revisión de procedimientos operativos**.

Análisis individual

Evalúa el desempeño y nivel de conocimientos de cada trabajador para detectar **necesidades de formación** personalizadas. Es clave para mejorar el desempeño en puestos específicos o tras cambios normativos.



Software de control de contratistas: 7 beneficios clave para tu empresa en 2025

En un escenario empresarial donde la seguridad, la eficiencia operativa y el cumplimiento normativo son prioritarios, muchas organizaciones se enfrentan al reto de conseguir una **gestión de contratistas** eficaz. Esta necesidad se complica en sectores con alta carga regulatoria o múltiples ubicaciones de trabajo. Un **software de control de contratistas** se convierte entonces en herramienta estratégica para garantizar una supervisión sistemática, reducir riesgos y optimizar recursos.

Contar con una solución digital especializada no solo **mejora la trazabilidad y la gestión documental**. También permite, entre muchas otras funciones, automatizar procesos, estandarizar flujos de trabajo y asegurar que los contratistas cumplan con todos los requisitos legales, formativos y de desempeño.

Además, puede integrarse con sistemas de gestión HSE como **ISO 45001** o ISO 14001. A continuación, exploramos las ventajas clave que un software de control de contratistas ofrece a las empresas que apuestan por una **gestión HSE moderna, proactiva y basada en datos**.

¿Qué ventajas tiene trabajar con un software de control de contratistas?

La **transformación digital** ha supuesto un enorme avance en la gestión HSE de las organizaciones, especialmente para aquellas que desarrollan parte de sus actividades apoyándose en fuerza laboral externa. **Los beneficios de un software de control de contratistas son numerosos**, pero entre ellos cabe destacar algunos:

1. Cumplimiento normativo garantizado

Uno de los mayores retos en la gestión de contratistas es asegurar que cada uno de ellos cumpla con los requisitos legales y normativos aplicables. Un software de control de contratistas **permite centralizar y validar documentación obligatoria** como licencias, certificados de formación en prevención de riesgos laborales o permisos de trabajo. Esa documentación no solo se almacena digitalmente, también se monitoriza en tiempo real. De esta manera, **se evitan sobrecostes, sanciones por incumplimiento** o paralización de actividades por no conformidades. Por otra parte, **cada acceso y cada actualización quedan registrados**. Este nivel de trazabilidad facilita **auditorías de salud y seguridad** y permite demostrar a auditores y entidades reguladoras que la gestión de contratistas de la organización es rigurosa y transparente.



Gestión digital de permisos de trabajo: pasos para optimizar el proceso

La **gestión digital de permisos de trabajo** responde a una necesidad creciente de las organizaciones. Se trata de un componente esencial, necesario para garantizar la seguridad en actividades de alto riesgo. Estos permisos conforman un sistema documentado que permite un control más eficiente y una mayor trazabilidad en la ejecución de tareas especialmente delicadas.

Tradicionalmente, los permisos de trabajo se han gestionado en papel, lo que conlleva desafíos significativos, como falta de trazabilidad, errores administrativos y dificultad para garantizar el cumplimiento normativo. La gestión digital de permisos de trabajo permite a las empresas **mejorar la eficiencia, reducir tiempos y garantizar la seguridad de las operaciones**.

¿Qué es un permiso de trabajo y por qué es crucial en HSE?

Un permiso de trabajo es un sistema de control documentado que **establece controles y requisitos específicos para la realización segura de tareas críticas**. Se utiliza principalmente en industrias con riesgos elevados, como construcción, química, energía o manufactura, además de en sectores donde ciertos trabajos requieren de medidas de seguridad estrictas y **elementos de protección personal**, por ejemplo:

- **Trabajos en espacios confinados:** operaciones en áreas con acceso restringido, riesgo de asfixia o acumulación de gases tóxicos.
- **Trabajos eléctricos en sistemas de alto voltaje:** procedimientos que requieren de medidas de aislamiento y verificación de seguridad para evitar descargas eléctricas.
- **Trabajos en caliente:** actividades que involucran fuentes de ignición como soldadura, corte o uso de materiales inflamables.

Estos permisos **regulan quién puede realizar las tareas, bajo qué condiciones** y qué medidas de seguridad deben aplicarse antes, durante y después de la ejecución del trabajo.

Proceso de gestión de permisos de trabajo paso a paso

La gestión de permisos de trabajo **sigue un proceso estructurado** para garantizar la seguridad y el cumplimiento normativo.



El papel del software para la gestión de seguridad y contratistas en la mejora del control de riesgos

Apostar por procesos manuales y evaluaciones subjetivas en la **gestión de contratistas** puede costar muy caro. No solo se compromete la seguridad operativa, sino que también se abren las puertas a sanciones, interrupciones en las operaciones e incluso a daños reputacionales difíciles de reparar. En ese escenario, apoyarse en un **software para la gestión de seguridad y contratistas** no es anticiparse al futuro, es responder a una necesidad real.

Las herramientas digitales diseñadas especialmente para este ámbito **permiten anticipar riesgos, garantizar el cumplimiento normativo y coordinar múltiples proveedores** en entornos cada vez más complejos. Frente a procesos manuales obsoletos, lentos y propensos al error, el software para la gestión de seguridad y contratistas se convierte en la única opción realmente efectiva.

Por qué la gestión tradicional de contratistas ya no es segura ni viable

Cuando las organizaciones siguen dependiendo de la **gestión manual**, de documentación en papel y comunicaciones informales, el margen de error se multiplica. El uso de nuevas tecnologías, el trabajo en remoto y la creciente dependencia de contratistas han generado exposición a **riesgos que requieren de enfoques de gestión más avanzados**. Un software para la gestión de seguridad y contratistas es la respuesta tecnológica a esta complejidad. Significa **pasar del enfoque reactivo al proactivo**, basado en información precisa, trazabilidad y eficiencia. Se superan así las **limitaciones impuestas por sistemas tradicionales**:

- ❖ **Retrasos en la comunicación** de incidentes por la dependencia de documentación en papel.
- ❖ **Errores humanos** en los procesos manuales de verificación de credenciales.
- ❖ **Información dispersa** que impide tomar decisiones informadas y coordinar de forma efectiva a los contratistas.
- ❖ **Falta de trazabilidad de la documentación**, que dificulta la respuesta inmediata ante situaciones de emergencia.

En definitiva, **los métodos reactivos resultan insuficientes** para gestionar la complejidad de los riesgos laborales en el entorno de las organizaciones modernas. Un software para la gestión de seguridad y contratistas se presenta entonces como una solución integral para anticipar, mitigar y auditar riesgos de forma sistemática.

EMERGENCY PLAN

Qué incluir en un plan de acción de emergencia en el lugar de trabajo

Disponer de un **plan de acción de emergencia** sólido como parte de los **programas HSE** es mucho más que un requisito normativo. Las organizaciones se enfrentan a infinidad de amenazas que pueden interrumpir bruscamente sus operaciones, desde incendios y fenómenos naturales hasta ciberataques. Son eventos con capacidad de ocasionar pérdidas económicas significativas, sin olvidar que pueden comprometer la seguridad de las personas.

Un plan de acción de emergencia es una herramienta estratégica que **articula la continuidad operativa, la protección del personal y la resiliencia organizacional**. Bien estructurado, identifica escenarios críticos, minimiza impactos y permite recuperar la actividad en el menor tiempo posible. De esta manera, un plan de acción de emergencia es el elemento que **marca la diferencia entre una respuesta coordinada y eficiente y otra improvisada**.

Además, para los especialistas en HSE, contar con protocolos de actuación robustos es una obligación recogida en normativas como **ISO 45001** (cláusulas 8.2 y 8.3) y directrices sectoriales específicas.

¿Qué es un plan de acción de emergencia?

Un plan de acción de emergencia **es un sistema integral de gestión de crisis**. Su diseño debe responder a las particularidades de cada organización, adaptándose tanto a su estructura física como a sus dinámicas operativas. **Su enfoque debe ser integral**. Significa que en él es imprescindible contemplar riesgos físicos, emergencias digitales, conflictos sociales o situaciones mixtas. También debe incluir a todos los actores posibles, desde trabajadores a visitantes que puedan desconocer los procedimientos de emergencias.

La eficacia de un plan de acción de emergencia radica en la **precisión con la que se anticipen escenarios críticos y se definan roles**, responsabilidades y recursos necesarios para minimizar el impacto de cualquier incidente. Esta es la forma de garantizar que el plan no sea simplemente un documento estático, sino una herramienta dinámica de gestión de crisis.

Componentes básicos de un plan de acción de emergencia

Un plan de acción de emergencia **puede variar según a actividad de la organización y los organismos reguladores**.



Cómo realizar un análisis de riesgos laborales para una evaluación eficaz

Una buena **gestión de riesgos laborales** no solo protege la integridad física de los trabajadores. También es esencial para sostener la operatividad de la organización, optimizar recursos y transmitir una imagen de responsabilidad frente a socios, inversores y empleados. En un entorno regulado y cada vez más exigente con la sostenibilidad, el **análisis de riesgos laborales** se convierte en un factor estratégico.

Identificar riesgos de seguridad y salud en el lugar de trabajo no es suficiente. El verdadero valor está en **anticiparse, priorizar lo crítico y adoptar medidas adaptadas al contexto real** de la organización. Por ello, un análisis de riesgos laborales requiere de un enfoque estructurado y a la vez flexible, apoyado en tecnología y cultura preventiva.

Las seis fases en un análisis de riesgos laborales

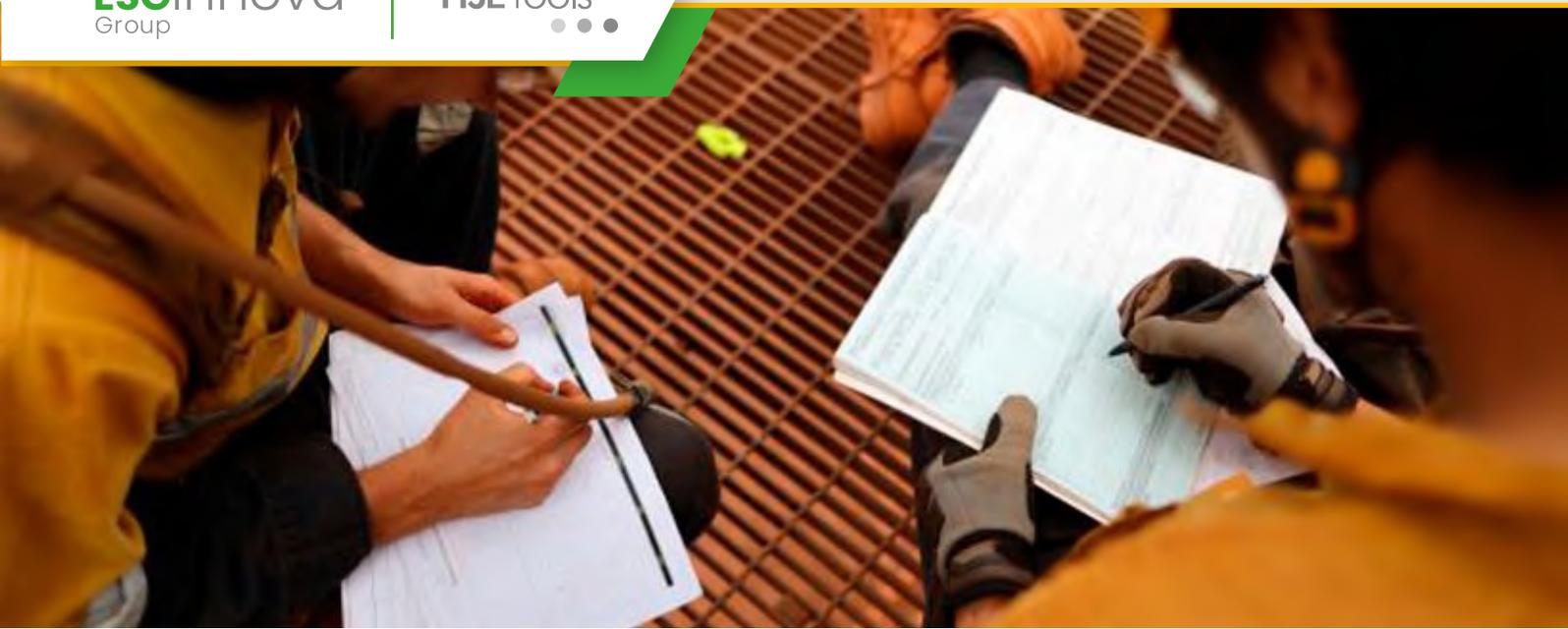
Ese **enfoque sistemático del análisis de riesgos laborales** es indispensable para cumplir con normativas internacionales como **ISO 45001** y garantizar la continuidad de las operaciones. Para ello, se requiere superar varias etapas:

1. Delimitar el alcance

Antes de lanzarse a identificar riesgos, hay que **definir claramente qué se va a analizar**: áreas físicas, procesos productivos, actividades o equipos objeto de evaluación. También conviene tener presente el contexto interno y externo, con aspectos que van desde la estructura organizativa a la competencia del personal o el entorno legal. La precisión en esta etapa determina la efectividad del proceso completo.

2. Identificar peligros, visibles y ocultos

Algunos riesgos son evidentes, otros no tanto. A veces surgen por la interacción entre procesos o por cambios en el entorno que han pasado desapercibidos. Por eso, además de observar el entorno de trabajo para detectar cualquier riesgo potencial de seguridad, hay que **hablar con los trabajadores, revisar registros históricos** y dedicar tiempo suficiente para entender bien el terreno. Esta fase **debe contemplar peligros físicos, químicos, biológicos y ergonómicos** presentes en el ambiente laboral, además de los **riesgos psicosociales**. Inspecciones directas, análisis documental, entrevistas con trabajadores y revisión de registros históricos permiten una identificación más precisa.



Formularios de notificación de incidentes de seguridad: qué datos deben incluirse

La **notificación de incidentes de seguridad** es un proceso de enorme relevancia dentro de los **planes de acción HSE**. Formularios bien diseñados son la primera línea de defensa para prevenir accidentes graves y garantizar el cumplimiento normativo, ya que permiten a las organizaciones identificar riesgos y tomar decisiones informadas.

Pese a ello, muchas empresas subestiman la importancia de diseñar formularios completos, que recojan la **información crítica necesaria para una reacción rápida y adecuada**. La ausencia de notificación de incidentes de seguridad puede costar a la organización severos daños económicos y reputacionales.

Qué debe contener un formulario eficaz de notificación de incidentes de seguridad

La diferencia entre un incidente menor y una crisis corporativa a veces radica en la calidad de los datos recopilados en el momento del reporte inicial. De ahí la importancia de **diseñar correctamente los formularios** de notificación de incidentes de seguridad.

1. Datos generales y contexto temporal

Todo formulario de notificación de incidentes de seguridad **debe incluir, entre otros, los siguientes datos:**

- 01.** Número de registro automático.
- 02.** Fecha y hora exactas del incidente y del reporte.
- 03.** Ubicación precisa, con posibilidad de geolocalización automática.

La precisión es clave para la **investigación de incidentes**, para establecer cronologías, identificar patrones y cumplir con plazos normativos.

2. Descripción estructurada del incidente

Es el núcleo del informe. **Debe reflejar qué y cómo ocurrió, causas aparentes y consecuencias inmediatas.** Un formulario bien estructurado ayuda a quienes deben informar para que proporcionen información completa sin omitir detalles críticos.

GRCTools



Transformación Digital
para la Gestión de
**Gobierno, Riesgo y
Cumplimiento**



Cómo afrontar los riesgos del RGPD en la Inteligencia Artificial

Pongamos sobre la mesa el contexto empresarial actual en torno a los riesgos del RGPD: la **automatización** y el uso de **tecnologías predictivas**, como la **Inteligencia Artificial (IA)**, se han consolidado como un motor de innovación. Sin embargo, este avance técnico plantea desafíos significativos para la **protección de datos personales**, especialmente en lo que respecta al cumplimiento del **Reglamento General de Protección de Datos (RGPD)**.

La IA depende de grandes volúmenes de información para generar patrones, tomar decisiones o anticipar comportamientos. Cuando esta información incluye datos personales —como hábitos de consumo, datos biométricos, ubicaciones o historiales clínicos—, surgen riesgos críticos que deben gestionarse con rigor. El incumplimiento del RGPD en proyectos de IA deriva en **sanciones económicas severas**, y también en una pérdida de **confianza pública** y en impactos éticos y reputacionales de gran alcance.

Riesgos del RGPD: La complejidad del cumplimiento en sistemas inteligentes

A diferencia de los sistemas tradicionales, los algoritmos de IA — especialmente los basados en **machine learning** o **deep learning**— presentan problemas de **opacidad**. Es frecuente que ni siquiera los desarrolladores puedan explicar con claridad cómo un modelo ha llegado a una decisión concreta, lo que dificulta garantizar los derechos reconocidos en el RGPD, como el derecho a la información, el acceso o la oposición.

Además, la IA suele requerir el tratamiento de **grandes volúmenes de datos**, lo que entra en tensión con principios como la **minimización del tratamiento** o la **limitación de la finalidad**. Esta situación obliga a las organizaciones a adoptar enfoques preventivos y estructurados para mitigar los riesgos y asegurar la **responsabilidad proactiva**.

Principales riesgos del RGPD en la IA

Entre los riesgos más relevantes que plantea el uso de IA en relación con el RGPD, destacan:

- **Falta de transparencia:** La naturaleza técnica de los modelos puede impedir a los usuarios comprender cómo y por qué se han utilizado sus datos.
- **Decisiones automatizadas sin intervención humana:** El artículo 22 del RGPD limita este tipo de decisiones cuando pueden tener efectos significativos sobre el interesado.
- **Perfiles discriminatorios:** Si los datos de entrenamiento están sesgados, el algoritmo puede reproducir o amplificar esa discriminación.



Evaluación de riesgos empresariales para la toma de decisiones

La **evaluación de riesgos empresariales** se ha convertido en una herramienta estratégica para garantizar la sostenibilidad y competitividad de las organizaciones. Las decisiones empresariales —desde la expansión a nuevos mercados hasta la incorporación de tecnologías disruptivas— ya no pueden tomarse sin un análisis riguroso de los factores que podrían poner en peligro los objetivos corporativos.

La capacidad para identificar, valorar y gestionar riesgos de forma anticipada no solo protege a la empresa frente a eventos adversos, también genera una ventaja competitiva.

La **gestión proactiva del riesgo** permite a las organizaciones anticiparse a los cambios regulatorios, responder a los movimientos del mercado y fortalecer la confianza de inversores, clientes y stakeholders.

Evaluación de riesgos empresariales: Una necesidad estratégica, no solo operativa

Tradicionalmente, el análisis de riesgos se asociaba a la seguridad operativa, el cumplimiento legal o la prevención de accidentes. Sin embargo, en la actualidad, la **evaluación de riesgos empresariales** ha evolucionado hacia una función transversal que abarca dimensiones financieras, reputacionales, tecnológicas, medioambientales y sociales.

El reto ya no es simplemente “cumplir”, sino **integrar la gestión de riesgos en el proceso de toma de decisiones**. Esto implica entender los riesgos no como amenazas aisladas, más bien pasar a verlos como elementos clave para priorizar inversiones, asignar recursos, rediseñar procesos y construir resiliencia organizacional.

¿Qué riesgos deben considerarse?

La variedad y complejidad de los riesgos empresariales obliga a las organizaciones a disponer de una visión estructurada. Algunos de los principales tipos de riesgo que deben evaluarse incluyen:

- **Riesgos estratégicos:** decisiones mal orientadas, inversiones fallidas, cambios en el modelo de negocio.
- **Riesgos financieros:** fluctuaciones en el tipo de cambio, impagos, inflación, acceso a financiación.
- **Riesgos operacionales:** fallos en procesos clave, interrupciones logísticas, dependencia de proveedores.



Cómo implementar programas ESG efectivos

El concepto de **sostenibilidad empresarial** ha cobrado una relevancia central en la gestión moderna. Cada vez más organizaciones integran los criterios ESG —ambientales, sociales y de gobernanza— como parte fundamental de su estrategia, reconociendo que estos factores influyen directamente en la capacidad de la empresa para adaptarse, crecer y generar valor en el tiempo.

El desafío actual ya no radica en justificar la necesidad de actuar, sino en **operativizar los compromisos ESG** de manera estructurada y eficaz. Implementar programas ESG efectivos implica transformar principios en acciones, definir indicadores claros, gestionar datos con precisión y alinear a toda la organización con objetivos comunes. Este proceso requiere método, liderazgo y tecnología, así como una escucha activa de los grupos de interés.

Fundamentos de implementar programas ESG efectivos

El punto de partida para implementar un programa ESG efectivo es llevar a cabo una **evaluación de materialidad**. Para implementar

programas ESG efectivos, es clave comenzar con una visión clara y una evaluación de materialidad bien estructurada. Este proceso permite identificar los aspectos ambientales, sociales y de gobernanza más relevantes para la empresa y sus grupos de interés. En él se analizan temas como consumo energético, emisiones, gestión de residuos, condiciones laborales, diversidad, relaciones con proveedores o la ética corporativa.

Una vez definidos los temas prioritarios, se deben establecer **indicadores clave de desempeño (KPIs)** y recoger datos que sirvan de línea base. ¿Cuáles son las emisiones actuales? ¿Qué porcentaje de mujeres hay en cargos directivos? ¿Se dispone de un código ético implementado y revisado periódicamente? Sin datos confiables, no hay posibilidad de mejora ni de comunicación transparente.

También es esencial involucrar a los **grupos de interés** desde el principio. La consulta con empleados, clientes, inversores o comunidades permite validar prioridades, detectar expectativas y fortalecer el compromiso con el programa.

ESG y estrategia empresarial: un solo camino para implementar programas ESG efectivos

Una de las claves para lograr que un programa ESG sea efectivo es evitar tratarlo como un proyecto aislado. En cambio, debe **integrarse en la estrategia y la operativa diaria** de la empresa. Las decisiones de inversión, las políticas internas, los procesos de innovación o la gestión de la cadena de suministro deben alinearse con los objetivos ESG establecidos. Las organizaciones que desean implementar programas ESG efectivos deben contar con herramientas que faciliten la recopilación de datos, el análisis de indicadores y la participación de los grupos de interés.



El camino hacia la Excelencia

Desde los inicios de nuestra organización han pasado más de quince años de trabajo y mejora continua, donde el desarrollo de alianzas, la ampliación en normas y modelos, el gran crecimiento en número de clientes y tipología de proyectos, así como la expansión internacional, han marcado y marcan nuestra trayectoria.

Estamos presentes en más de quince países, en los que nuestros equipos locales prestan un servicio adaptado a la realidad y mercado de cada zona.

+2.500
organizaciones

+25
años

+30
países

+240.000
usuarios

ESGinnova

Group

Córdoba, España

C. Villnius N° 15, P.I. Tecnocórdoba,
Parcela 6-11 Nave H, 14014
Tel: +34 957 102 000

Écija, España

Avda. Blas Infante, 6, Sevilla
Écija - 41400
Tel: +34 957 102 000

Santiago de Chile, Chile

Avda. Providencia 1208,
Oficina 202
Tel: +56 2 2632 1376

Lima, Perú

Avda. Larco 1150,
Oficina 602, Miraflores
Tel: +51 987416196

Bogotá, Colombia

Carrera 49,
N° 94 - 23
Tel: +57 601 3000590 | +57 320 3657308

México DF, México

Av. Darwin N°. 74, Interior 301,
Colonia Anzures, Ciudad de México
11590 México
Tel: +52 5541616885

