EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

2025

OCTUBRE

ESGinnova Group

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

Índice

Índice

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.

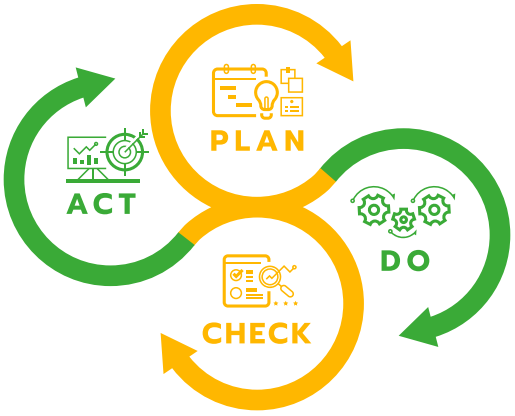
Plataforma ESG Innova

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

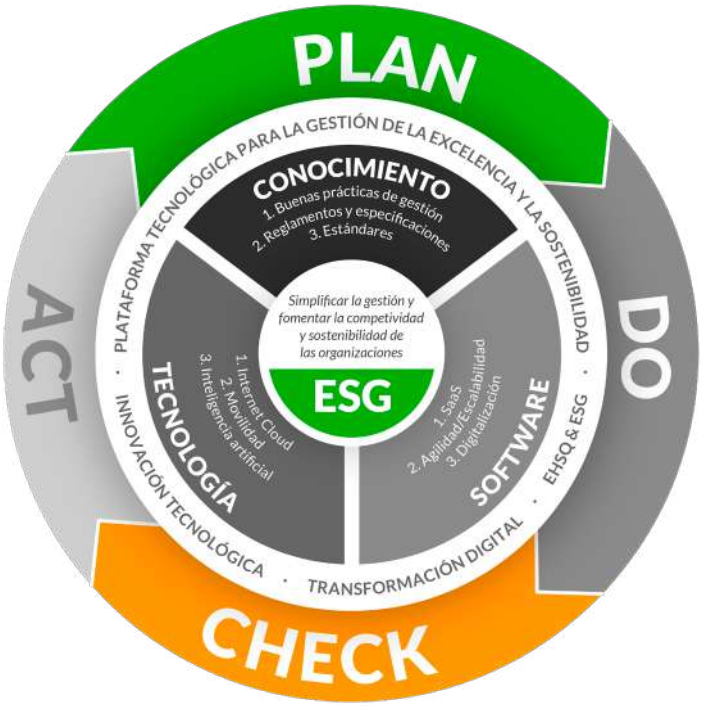
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ 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

50%
Menos de tiempo de resolución de una acción correctiva

20%
Menos de tiempo de preparación de las reuniones de gestión

75%
Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

90%
Menos de intercambios de documentación física entre sedes y dptos.

75%
Menos de costes indirectos derivados de la gestión documental

ROI
1-2 AÑOS
La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento

25%
Más de optimización en el sistema de gestión tras la etapa de consultoría

4
VECES
Más capacidad de resolución de problemas del sistema de gestión

100%
Más de trabajadores implicados en la gestión del sistema

ESGinnova Group

ISOTools

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

¿Cuál es la diferencia entre ISO 9000 y 9001?

A menudo, cuando una organización comienza a interesarse por la gestión de la calidad, surge la misma duda: **¿cuál es la diferencia entre ISO 9000 e ISO 9001?**

Ambas pertenecen a la **familia de normas ISO 9000**, un conjunto de estándares internacionales desarrollados por la Organización Internacional de Normalización (ISO) que promueven la **mejora continua, la eficiencia operativa y la satisfacción del cliente**.

Sin embargo, aunque estén relacionadas, **ISO 9000** e **ISO 9001** cumplen **funciones distintas** dentro del sistema. Mientras **ISO 9000** explica **los fundamentos y el vocabulario** de la gestión de la calidad, **ISO 9001** establece **los requisitos certificables** para implantar un **Sistema de Gestión de la Calidad (SGC)**. En otras palabras, **ISO 9000 enseña los conceptos**, e **ISO 9001 los pone en práctica**.

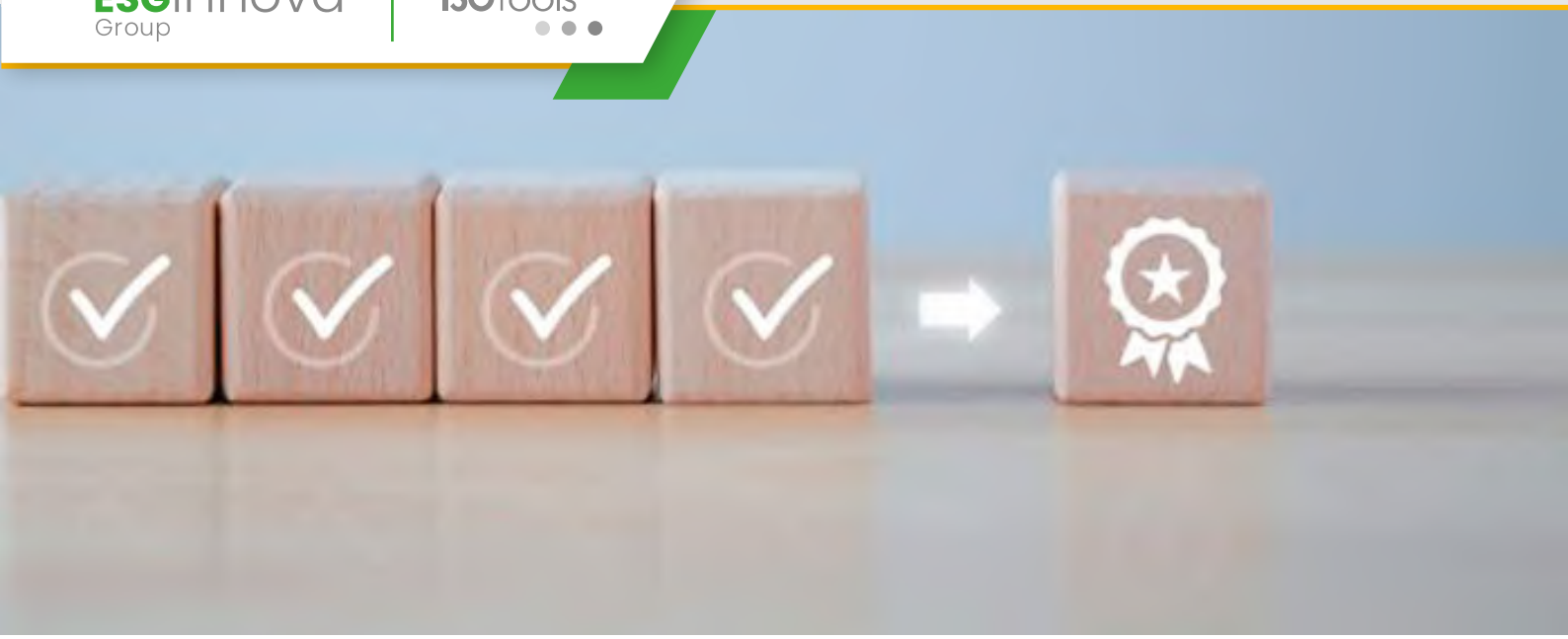
ISO 9000: fundamentos, vocabulario y principios de la calidad

La **norma ISO 9000:2015** es la base conceptual del sistema de gestión de la calidad. Su objetivo es **definir con precisión los términos y principios** que sustentan la gestión de la calidad moderna. No se trata de una norma que establezca requisitos, sino de una **guía teórica y terminológica** que permite a las organizaciones comprender qué significa realmente gestionar con calidad.

Diferencia entre ISO 9000 y 9001: principios en los que se basa la norma ISO 9000

ISO 9000 establece **siete principios de gestión de la calidad** que orientan la toma de decisiones y el diseño del sistema:

- **Enfoque al cliente:** satisfacer y superar las expectativas del cliente.
- **Liderazgo:** la dirección establece unidad de propósito y compromiso.
- **Compromiso de las personas:** la calidad se construye con la implicación de todos.
- **Enfoque a procesos:** entender y gestionar actividades interrelacionadas como un sistema coherente.
- **Mejora continua:** base del progreso organizacional sostenido.
- **Toma de decisiones basada en evidencia:** utilizar datos y hechos para decidir.



ISO 45001:2027: actualización de la norma de seguridad y salud en el trabajo

La Organización Internacional de Normalización prepara una actualización de ISO 45001. Esta nueva versión del estándar representa una evolución significativa en la gestión de la salud y seguridad laboral. Con **ISO 45001:2027** se busca fortalecer la protección de los trabajadores ante desafíos emergentes como los riesgos psicosociales, la diversidad organizacional y los impactos del cambio climático en el trabajo.

Anticipar estos cambios es fundamental para las organizaciones que buscan mantener sus sistemas de gestión a la vanguardia. **Conocer las líneas maestras que guiarán la nueva ISO 45001:2027 permite planificar una transición ordenada**, minimizar impactos operativos y transformar la actualización normativa en una oportunidad para mejorar la **gestión de la salud y seguridad en el trabajo** de manera sustancial.

¿Por qué se actualiza ISO 45001?

El entorno laboral ha experimentado transformaciones significativas desde la publicación de la ISO 45001 en 2018. Los cambios se justifican por la **necesidad de la norma de reflejar un contexto global que ya no se limita a los riesgos físicos tradicionales**, sino que abarca la complejidad de los entornos laborales modernos.

ISO 45001:2027 surge así por la necesidad de garantizar que la salud y seguridad laboral no solo prevenga accidentes, sino que también **promueva un bienestar integral y se adapte a las nuevas herramientas de gestión**. La actualización es fundamental por diferentes motivos:

- **Mejorar la seguridad de los trabajadores**: al incorporar una gestión de riesgos proactiva y una mayor participación de los trabajadores, la norma contribuye a prevenir accidentes y lesiones.

- **Impulsar el desempeño empresarial**: una fuerza laboral segura y saludable es más productiva. ISO 45001:2027 busca ayudar a las organizaciones a reducir el tiempo de inactividad, mejorar la eficiencia operativa y fortalecer su reputación.

- **Promover una cultura de bienestar**: la inclusión de la salud mental y el bienestar fomenta un entorno laboral más positivo y de apoyo, reduciendo el estrés y mejorando la moral de los empleados.

- **Asegurar el cumplimiento**: la adhesión al estándar actualizado demuestra un compromiso con las mejores prácticas en SST, ayudando a las organizaciones a cumplir con los requisitos legales y regulatorios.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Auditoría de TI: guía práctica de 7 pasos para asegurar el cumplimiento

En un entorno donde los datos son el activo más valioso de las organizaciones y las amenazas cibernéticas evolucionan sin cesar, la auditoría de TI es una herramienta esencial para evaluar la madurez tecnológica y garantizar la seguridad de la información. Normas como **ISO 27001** proporcionan un marco sólido para proteger la confidencialidad, integridad y disponibilidad de los datos, pero alcanzar y mantener el cumplimiento exige un proceso sistemático de revisión y mejora continua.

Auditar los sistemas de información se ha convertido así en un ejercicio estratégico. Permite detectar vulnerabilidades antes de que se conviertan en incidentes y fortalece la confianza entre clientes, proveedores y socios. Sin embargo, preparar y ejecutar una auditoría de TI requiere planificación, coordinación y metodología.

Qué es una auditoría de TI

Una auditoría de TI **es una evaluación estructurada de los procesos, controles y recursos tecnológicos** de una organización. Su objetivo es comprobar si las prácticas implementadas cumplen con los requisitos internos, las políticas de seguridad y estándares internacionales como ISO 27001.

A través de esta auditoría, que **puede ser interna o externa**, se revisa cómo se gestionan los activos tecnológicos, cómo se protege la información y hasta qué punto son eficaces las medidas de seguridad aplicadas. Además, permite identificar brechas de cumplimiento, proponer acciones correctivas y optimizar los procesos que sostienen un **Sistema de Gestión de Seguridad de la Información** (SGSI).

Quién necesita una auditoría de TI

Toda organización que dependa de la tecnología para operar, proteger datos u ofrecer servicios digitales debe realizar auditorías periódicas de cumplimiento de TI. En sectores altamente regulados, estas evaluaciones son obligatorias, especialmente en:

- Empresas que gestionan datos personales o financieros.
- Organizaciones certificadas o que buscan certificarse en normas ISO.
- Entidades públicas y privadas con infraestructuras críticas o servicios en la nube.
- Proveedores de servicios SaaS o empresas con entornos digitales complejos.

Transición de AS9100 a IA9100: actualización y qué esperar

La Transición de AS9100 a IA9100 representa uno de los cambios más importantes en la historia reciente de la **industria aeroespacial, de aviación y defensa**. El **International Aerospace Quality Group (IAQG)**, organismo responsable de los estándares de **calidad** del sector, ha impulsado esta actualización con el objetivo de **unificar, modernizar y fortalecer** los requisitos de gestión de la calidad a nivel global.

La nueva **IA9100** no solo sustituye a la AS9100, sino que **introduce un marco más robusto, digital y sostenible**, adaptado a los desafíos actuales de la industria, como la ciberseguridad, la sostenibilidad y la gestión avanzada de la calidad. Su publicación oficial está prevista para finales de **2025 o inicios de 2026**, y marcará un antes y un después en la forma de gestionar la calidad en el sector aeroespacial.

AS9100: la base del sistema de calidad aeroespacial

La **AS9100** es la norma que, durante más de dos décadas, ha guiado los sistemas de gestión de la calidad en la industria aeroespacial. Basada en la **ISO 9001**, esta norma añade **requisitos específicos** que garantizan la **seguridad, confiabilidad y trazabilidad** en el diseño, fabricación y mantenimiento de productos aeronáuticos y espaciales.

Además de la AS9100, la familia de normas AS incluye:

- **AS9110**, dirigida a organizaciones de mantenimiento y reparación (MRO).
- **AS9120**, orientada a distribuidores y empresas de suministro de componentes.
- Gracias a estas normas, el sector ha logrado **homogeneizar sus procesos**, reducir errores, aumentar la seguridad y consolidar una cultura de calidad reconocida internacionalmente.

Sin embargo, el entorno tecnológico, las amenazas digitales y los nuevos compromisos medioambientales han impulsado la necesidad de evolucionar hacia un **modelo de gestión más moderno, global y sostenible**: **IA9100**.

IA9100: la evolución natural de la calidad aeroespacial

La futura **IA9100** se presenta como una **actualización integral** que refuerza los principios de la AS9100, integrando nuevas dimensiones críticas para la gestión moderna. Además, su propósito principal es **unificar las normas AS** bajo una **identidad global coherente**, alineada con los desafíos contemporáneos de la industria.

Gestión de inteligencia artificial: cómo ISO 42001 establece un marco global

La rápida adopción de sistemas de IA plantea grandes desafíos relacionados con la ética, transparencia y seguridad que requieren marcos estructurados. La gestión de inteligencia artificial se ha convertido así en una prioridad para muchas organizaciones. La norma **ISO 42001** propone un modelo estructurado que permite implementar un sistema de gestión de la IA (SGIA) capaz de garantizar un uso responsable y alineado con los objetivos empresariales.

Más que una guía técnica, ISO 42001 es una herramienta para consolidar la **gobernanza de la IA** promoviendo la transparencia, la rendición de cuentas y la mejora continua en todo su ciclo de vida. Este estándar internacional ofrece a las organizaciones un modelo flexible que **permite aprovechar las ventajas de la IA mientras se gestionan sus riesgos** de forma sistemática.

¿Por qué establecer un marco para la gestión de inteligencia artificial?

El desarrollo acelerado de la inteligencia artificial ha traído consigo beneficios, pero también retos como sesgos algorítmicos, uso indebido de datos o impactos sociales no previstos. Disponer de una norma que estructure su gestión permite a las organizaciones **anticiparse a estos riesgos y demostrar compromiso con la responsabilidad digital**.

ISO 42001 propone un sistema de gestión de inteligencia artificial que **sigue la estructura armonizada de las normas ISO**. Esto facilita su integración con otros estándares como **ISO 27001** (seguridad de la información) o ISO 27701 (privacidad), asegurando coherencia en los procesos organizativos.

El SGIA abarca todo el ciclo de vida de la IA, desde la planificación y el diseño hasta la implementación, operación, evaluación y mejora continua. Además, al ser certificable, ofrece credibilidad y facilita la confianza de socios, clientes y reguladores.

Estructura del sistema de gestión de inteligencia artificial según ISO 42001

La norma establece requisitos de alto nivel que guían a las organizaciones en la creación de su **sistema de gestión de IA**:

- **Contexto de la organización**: ISO 42001 exige comprender el entorno, los factores internos y externos, así como las necesidades de las partes interesadas. Es necesario, además, establecer su alcance.

Sistema de gestión de calidad ISO 9001: beneficios más allá de la certificación

Implementar un sistema de gestión de calidad (SGC) basado en **ISO 9001** es una decisión que impacta en todas las áreas de una organización. Más que un conjunto de requisitos normativos, se trata de un modelo de gestión que impulsa la excelencia, la eficiencia y la confianza del cliente. Además, genera valor tangible en toda la cadena operativa.

ISO 9001 ofrece un **marco integral para estructurar operaciones centradas en el cliente** basadas en un liderazgo efectivo, en la mejora continua y en decisiones fundamentadas en datos. Comprender sus beneficios reales permite a las organizaciones maximizar la inversión y convertir la gestión de calidad en una ventaja competitiva sostenible. Pero los beneficios de este sistema van mucho más allá de obtener la **certificación ISO 9001**.

¿Por qué implantar un sistema de gestión de calidad ISO 9001?

Adoptar un sistema de gestión de calidad normalizado **permite estandarizar procesos, fortalecer la toma de decisiones** y alinear a toda la organización en torno a un objetivo común: la **satisfacción del cliente**. ISO 9001 establece un marco flexible que puede aplicarse a organizaciones de cualquier tamaño o sector, desde la manufactura hasta los servicios o la tecnología.

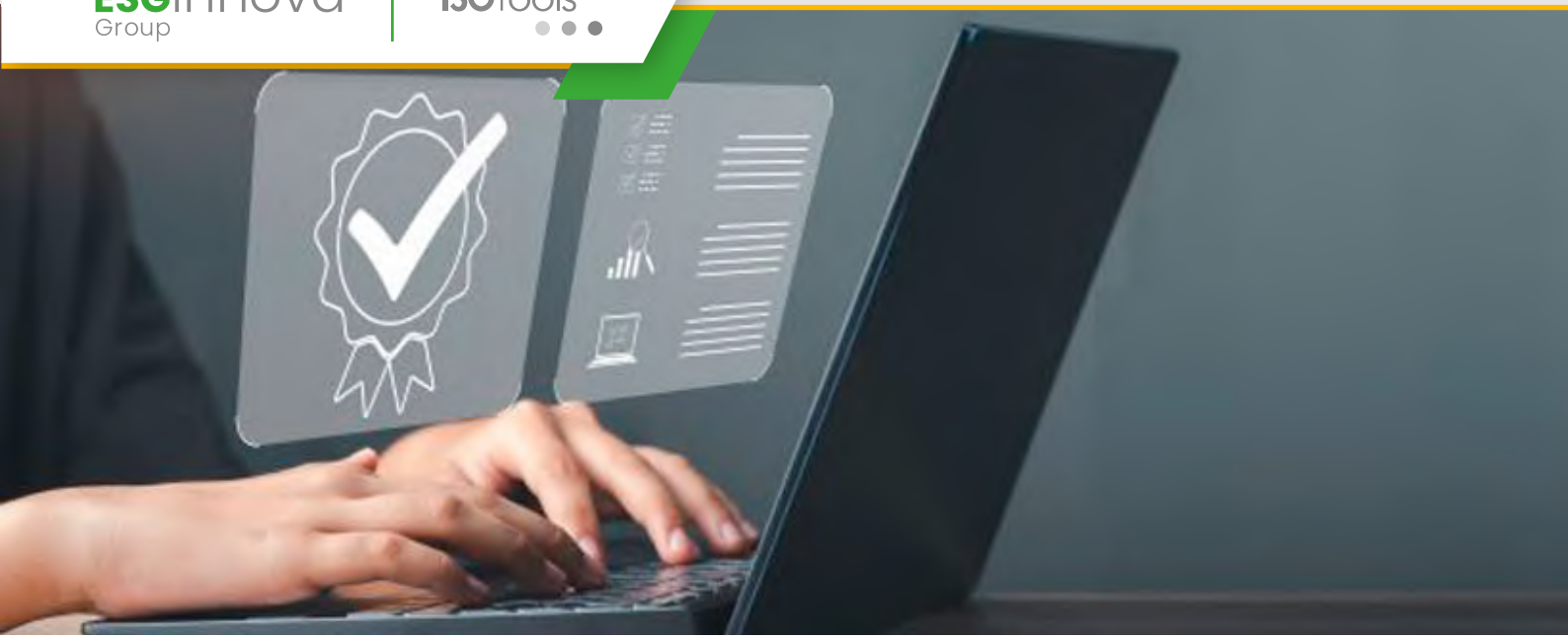
Por otra parte, el sistema de gestión de calidad es una herramienta esencial para **mejorar las tasas de crecimiento, rentabilidad y supervivencia de la organización**. Implementar un SGC no solo mejora la calidad del producto o servicio, sino que también genera un retorno tangible de la inversión.

Beneficios tangibles de un sistema de gestión según ISO 9001

Los beneficios cuantificables de un sistema de gestión de calidad permiten justificar la inversión ante cualquier nivel organizacional. Estos resultados **se reflejan directamente en indicadores financieros, métricas operativas y reducción de riesgos regulatorios**. Cada aspecto del sistema genera valor medible que impacta positivamente en la cuenta de resultados de la organización.

Consistencia operativa y eficiencia

La estandarización de procesos es la base de la calidad. Con un sistema bien diseñado, la organización **reduce la variabilidad, evita errores y garantiza resultados previsibles**.



Quién necesita ISO 42001: cómo saber si tu organización debería certificar su gestión de IA

La inteligencia artificial ha dejado de ser una tendencia para convertirse en una realidad operativa en las organizaciones. Pero con su adopción acelerada surgen algunas dudas, especialmente quién necesita **ISO 42001** y cuándo es el momento de certificar su gestión de IA. Aunque no existe legislación global que obligue a ello explícitamente, el mercado se ha adelantado a los reguladores, imponiendo estándares que trascienden los requisitos legales.

La brecha entre la regulación y la práctica empresarial es el factor determinante. Clientes, aseguradoras e inversores han redefinido sus criterios de confianza, convirtiendo ISO 42001 en una exigencia. Para las organizaciones, entender cuándo y por qué necesitan esta certificación es crucial para evitar perder contratos, resolver obstáculos regulatorios y mantener la credibilidad en un mercado cada vez más exigente.

¿Por qué ISO 42001 es una necesidad estratégica?

No existe una legislación específica que obligue a la certificación ISO 42001 para implementar o adquirir soluciones de IA. Incluso la **Ley de IA de la UE**, el marco regulatorio más estricto, solo hace referencia genérica a sistemas de gestión sin especificar una norma concreta. Esto genera una falsa sensación de seguridad.

Aunque la certificación sea técnicamente voluntaria, **las fuerzas del mercado han convertido esta opción en un requisito de facto**. Las solicitudes de propuestas, las auditorías internas, los requisitos de seguros y los criterios de debida diligencia de inversores exigen ya demostraciones verificables de **gobernanza de IA**, no solo declaraciones de intenciones.

La norma **ISO 42001 define los requisitos para establecer, implementar y mantener sistemas de gestión de inteligencia artificial**. En la práctica, no contar con ella puede significar pérdida de contratos, cobertura y reputación. Por eso, entender quién necesita ISO 42001 se ha vuelto una prioridad para cualquier organización que trabaje con la nueva tecnología.

Quién necesita ISO 42001: sectores donde es imprescindible

El cumplimiento de ISO 42001 es especialmente **relevante para organizaciones que gestionan riesgos elevados o manejan grandes volúmenes de datos sensibles**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Resumen completo de la norma ISO 50001

La energía es hoy uno de los activos más críticos para la competitividad empresarial. Optimizar su uso exige una gestión estructurada, basada en datos y orientada a resultados. Con este propósito, la **ISO 50001** establece un estándar internacional que permite implantar y mejorar de forma constante un **Sistema de Gestión de la Energía (SGE)**, alineado con la estrategia global de la organización.

A continuación se presenta un resumen completo que abarca su propósito, estructura, principales requisitos, beneficios, y claves para su implantación.

¿Qué es la ISO 50001 y cuál es su objetivo?

La ISO 50001 es un estándar internacional desarrollado por la International Organization for Standardization (ISO) que proporciona un marco de referencia para establecer, implementar, mantener y mejorar un SGE, con el objetivo de mejorar el **desempeño energético**, incluyendo la eficiencia, el uso y el consumo de energía.

En esencia, la norma busca que las organizaciones puedan:

- Desarrollar una **política energética** orientada al uso eficiente de la energía.
- Fijar **objetivos y metas energéticas** que permitan alcanzar esa política.
- Analizar datos de consumo para tomar decisiones informadas sobre el uso de la energía.
- Medir resultados y revisar su desempeño energético.
- Mejorar continuamente el sistema y los resultados energéticos.
- Gracias a su estructura basada en la filosofía del ciclo **Plan-Do-Check-Act (PDCA)**, la norma es compatible e integrable con otros sistemas de gestión como la ISO 90001 o la ISO 14001.

Edición vigente y estructura de la norma

La edición actualmente vigente es la **ISO 50001:2018**, la cual incorpora mejoras en términos de alineación con otros sistemas de gestión y refuerza el enfoque en el desempeño energético. Respecto a su estructura, incluye los apartados típicos para un sistema de gestión, adecuados para cualquier tamaño de organización y sector.

Algunos de los capítulos clave son:

- Contexto de la organización, incluyendo la comprensión del entorno y de las partes interesadas.

Auditar a la alta dirección nueva ISO 9001:2026

La norma ISO 9001:2026 (en desarrollo) refuerza el papel estratégico de la **alta dirección** dentro del sistema de gestión de la calidad (SGC). Lejos de limitarse a una firma de compromiso, la alta dirección debe evidenciar **liderazgo activo**, fomentar una **cultura de calidad y ética**, integrar la **digitalización** y la **resiliencia operativa**, y demostrar su impacto en el desempeño global. Para los auditores internos y externos, este cambio supone una revisión profunda de los criterios de evaluación y de la forma de auditar este perfil clave en la organización.

1. ¿Por qué la alta dirección cobra mayor protagonismo?

La versión vigente, ISO 9001:2015, ya incluye requisitos en la cláusula de liderazgo, pero la revisión hacia la ISO 9001:2026 anticipa un salto cualitativo. Entre los principales cambios proyectados están: un énfasis más fuerte en la **cultura de calidad y comportamiento ético** vinculados directamente a la alta dirección, así como una mayor conexión con la **sostenibilidad**, los **riesgos emergentes**, la digitalización y la cadena de suministro.

Esto implica que la alta dirección ya no es únicamente responsable de aprobar la política de calidad, sino de liderar el sistema, promover su integración en la estrategia empresarial y asumir la responsabilidad por el desempeño global del SGC.

2. ¿Qué aspectos de la alta dirección debe auditar el sistema?

Para auditar eficazmente a la alta dirección bajo la norma ISO 9001:2026 es necesario centrar la evaluación en varios aspectos clave:

- **Compromiso y liderazgo visible**: La alta dirección debe demostrar su implicación en el SGC, asignar recursos, participar en revisión por la dirección y fomentar la mejora continua.

- **Política de calidad alineada con la estrategia**: La política debe reflejar la dirección de la organización, incluir objetivos de calidad, sostenibilidad y digitalización, y estar comunicada a todos los niveles.

- **Cultura de calidad y ética**: La norma anticipa requisitos explícitos para promover una cultura organizacional que impulse los valores de calidad, ética y comportamiento responsable. **Alisios Consultores+1**

- **Gestión de riesgos, oportunidades y resiliencia**: La alta dirección debe supervisar que el SGC no sólo gestione riesgos tradicionales, sino también amenazas emergentes (ciberseguridad, disrupciones de cadena de suministro, cambios regulatorios) e identifique oportunidades que fortalezcan la organización.

Guía completa de la Directiva DORA: requisitos, impacto y pasos para cumplirla

La **Directiva DORA**, la Ley de Resiliencia Operativa Digital de la Unión Europea, es una de las regulaciones más relevantes de los últimos años para el sector financiero. Su propósito es fortalecer la ciberresiliencia de las entidades y garantizar la continuidad de los servicios esenciales ante incidentes tecnológicos o ciberataques. En su espíritu, guarda relación con marcos como **ISO 27001**, que promueven la gestión sistemática de la seguridad de la información.

Con su aplicación obligatoria desde enero de 2025, la Directiva DORA redefine la manera en que las organizaciones abordan la ciberseguridad. **Supone pasar de un enfoque reactivo a una gestión proactiva del riesgo digital**, con obligaciones específicas sobre gobernanza, monitorización, respuesta a incidentes y control de proveedores tecnológicos.

Qué es la Directiva DORA y cuál es su propósito

La Directiva DORA nace como respuesta al aumento de **incidentes de ciberseguridad** y a la creciente dependencia tecnológica de las operaciones financieras. Su propósito central es **garantizar que las entidades financieras sean capaces de resistir, responder y recuperarse** de cualquier interrupción digital, fortaleciendo así la estabilidad del sistema financiero europeo. Entre sus principales objetivos se encuentran:

- **Fortalecer la ciberseguridad** mediante la adopción de controles técnicos y organizativos avanzados, que permitan anticipar, detectar y mitigar incidentes con rapidez.
- **Unificar estándares y requisitos** en toda la UE, eliminando la fragmentación normativa y creando un lenguaje común sobre resiliencia digital.
- **Asegurar la continuidad operativa**, promoviendo la planificación y la recuperación rápida tras interrupciones críticas.
- **Impulsar la cooperación** entre entidades y autoridades, permitiendo respuestas coordinadas ante amenazas de gran impacto.

¿A quién afecta la Directiva DORA?

La Directiva DORA **tiene un alcance amplio** y afecta tanto a las entidades financieras tradicionales como a **empresas tecnológicas** que prestan servicios esenciales al sector.

¿Qué incluye el Código de Prácticas de IA de Uso General de la Nueva Ley de IA de la UE?

El **Código de Prácticas de IA de Uso General** de la Ley de IA de la Unión Europea establece un marco de referencia voluntario que guía a los proveedores de modelos de inteligencia artificial de propósito general hacia un cumplimiento responsable y ético. Su aplicación está estrechamente vinculada a la norma **ISO 42001**, que proporciona la estructura necesaria para implementar un sistema de gestión de IA conforme a los principios de transparencia, seguridad y confianza.

Este código marca un paso decisivo en la madurez regulatoria de la inteligencia artificial en Europa. Nace como una herramienta práctica para **alinear los desarrollos tecnológicos con la legislación**, fomentando la gestión del riesgo y la protección de derechos fundamentales en un entorno digital cada vez más complejo.

Qué es el Código de Prácticas de IA de Uso General

El Código de Prácticas de IA de Uso General es una **guía voluntaria para los proveedores de modelos de inteligencia artificial de propósito general** y aquellos con riesgo sistémico. Su objetivo es facilitar el cumplimiento de los artículos 53 y 55 de la **Ley de Inteligencia Artificial de la UE**, anticipando la aplicación total de la normativa prevista para 2027.

Aunque su adhesión no constituye prueba definitiva de cumplimiento, sí **representa un compromiso verificable con las buenas prácticas en IA responsable**. El Código se articula en tres capítulos esenciales (transparencia, derechos de autor y seguridad) que reflejan las dimensiones clave de un uso confiable y ético de la tecnología.

Transparencia: la base de la confianza en la IA

El primer capítulo del Código de Prácticas de IA de Uso General **se centra en la documentación y trazabilidad de los modelos de IA**. Los proveedores deben mantener actualizada toda la información relativa al entrenamiento, arquitectura, limitaciones y propósito de uso de los modelos de propósito general.

Se incluye un formulario que especifica qué información debe compartirse con la Oficina de IA de la Unión Europea o con las autoridades nacionales, garantizando la protección de la confidencialidad según el artículo 78 de la Ley.

Este enfoque **fomenta una transparencia responsable**, suficiente para la supervisión regulatoria y, a la vez, respetuosa con la propiedad intelectual y la seguridad de los modelos.

Requisitos de ISO 14001: guía completa para implementar un sistema de gestión ambiental

La norma **ISO 14001** establece los requisitos para implantar un Sistema de Gestión Ambiental (SGA) eficaz, que permita a las organizaciones mejorar su desempeño ambiental y cumplir sus obligaciones legales. Comprender los **requisitos de ISO 14001** es, por ello, imprescindible si el objetivo es implementar un sistema sólido, capaz de prevenir riesgos, aprovechar oportunidades y contribuir a un desarrollo sostenible.

ISO 14001 proporciona un marco estructurado para gestionar los impactos ambientales. Su enfoque basado en procesos y mejora continua ayuda a las organizaciones a optimizar recursos, reducir costes y demostrar su compromiso con la sostenibilidad ante clientes, autoridades y la sociedad.

A continuación, analizamos de forma práctica y estructurada los principales requisitos de ISO 14001, cómo se aplican y qué documentación o evidencias se necesitan para cumplirlos con éxito.

Qué exige ISO 14001 a las organizaciones

La norma **se basa en el ciclo PDCA de mejora continua** y se estructura en diez cláusulas. Entre ellas, las cláusulas 4 a 10 son de carácter operativo y contienen los requisitos de ISO 14001 que deben implementarse y mantenerse documentados.

Estos requisitos buscan garantizar que el **sistema de gestión ambiental** (SGA) **esté integrado en la estrategia empresarial**, promueva la eficiencia en los procesos y reduzca el impacto ambiental de las actividades.

Alcance y contexto del sistema de gestión ambiental

Antes de definir políticas o procedimientos, **la organización debe establecer los límites de su sistema y comprender su entorno**. Este análisis permite adaptar el SGA a la realidad operativa, evitando duplicidades y garantizando la coherencia con la estrategia empresarial.

Definir el alcance del SGA

El primer paso imprescindible para cumplir con los requisitos de ISO 14001 consiste en determinar los límites y el alcance operativo del SGA. **La organización debe identificar qué procesos, ubicaciones, productos y servicios están incluidos**, así como las áreas que puedan quedar excluidas por motivos justificados. Este alcance debe documentarse y mantenerse actualizado.

Shadow AI: qué es, por qué representa un riesgo y cómo gestionarla eficazmente

Shadow AI reproduce en el ámbito de la inteligencia artificial los dilemas que hace años generó el uso de tecnología en la sombra. Muchos empleados incorporan herramientas de IA en su trabajo diario sin autorización corporativa. Les impulsa la búsqueda de eficiencia, pero no siempre miden los riesgos, lo que genera brechas de seguridad. Frente a esta realidad, marcos como **ISO 42001** favorecen una gestión segura, ética y trazable de la inteligencia artificial.

Si por algo se caracteriza Shadow AI es por su facilidad de adopción y su aparente inocuidad. Basta con acceder a un chatbot o a una plataforma generativa para que la información sensible pueda salir del perímetro corporativo. Así, la frontera entre el uso legítimo y el uso riesgoso se difumina, lo que obliga a las organizaciones a equilibrar la innovación con la seguridad, integrando la inteligencia artificial bajo principios de responsabilidad y control.

Shadow AI: un fenómeno que se expande en silencio

El uso no autorizado de herramientas de inteligencia artificial ha dejado de ser una excepción para convertirse en una práctica habitual en el entorno corporativo. Los datos recopilados por organizaciones especializadas en ciberseguridad revelan una extensión del fenómeno que supera todas las previsiones. **Entender la dimensión del alcance de este fenómeno resulta fundamental para diseñar estrategias de mitigación efectivas**.

Presencia masiva en las infraestructuras corporativas

Investigaciones recientes demuestran la rápida evolución del fenómeno Shadow AI. En su análisis de 2025, **Check Point Research** refleja que al menos el 50% de las infraestructuras empresariales registran actividad mensual en servicios de IA.

Por su parte, un **estudio de Cyberhaven Labs** señala que el volumen de datos transferidos a estas plataformas se ha multiplicado por cinco en apenas un año. Esta penetración masiva ocurre en muchos casos **sin conocimiento ni supervisión de los responsables de seguridad de la organización**.

Con frecuencia, los empleados acceden a sistemas de Shadow AI mediante cuentas personales o desde navegadores no monitorizados, lo que elimina capas críticas de protección.

Esta exposición afecta a información de clientes, documentación técnica, proyectos en desarrollo o registros financieros. Comprender la magnitud del problema es esencial para diseñar estrategias de mitigación realistas.

ESGinnova
Group

HSE Tools

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

Predicción de incidentes de seguridad: cómo la IA está transformando la prevención en el trabajo

Prevenir accidentes laborales es un objetivo prioritario para las organizaciones y, en esta tarea, el desarrollo tecnológico ha abierto nuevos horizontes. La predicción de incidentes de seguridad ya no es un concepto futurista, es una realidad que permite a las empresas anticiparse a riesgos antes de que puedan materializarse. Gracias a la inteligencia artificial, la **gestión de incidentes y accidentes** ha dado un paso de gigante.

En un contexto donde las exigencias regulatorias son cada vez más estrictas y los entornos de trabajo más complejos, **la IA se convierte en un aliado estratégico**. Detectar patrones invisibles al ojo humano, generar alertas en tiempo real o automatizar informes son solo algunas de las aplicaciones que están revolucionando la **gestión de la prevención de riesgos**.

Predicción de incidentes de seguridad: un nuevo paradigma

El concepto de predicción de incidentes de seguridad supone **pasar de un modelo reactivo, centrado en responder tras un accidente, a uno proactivo**, en el que se identifican señales tempranas y se aplican medidas antes de que ocurra un evento. **La IA utiliza datos históricos de incidentes, condiciones ambientales, registros de comportamiento y sensores IoT** para detectar correlaciones y anticipar riesgos. De esta forma, las organizaciones no solo cumplen con la normativa, sino que logran reducir la siniestralidad y aumentar la confianza de los trabajadores y otras partes interesadas.

Del análisis reactivo a la anticipación proactiva

La gestión tradicional de la seguridad laboral se ha basado en respuestas posteriores al incidente. Sin embargo, mediante el análisis de datos históricos y en tiempo real, **los algoritmos de IA pueden predecir posibles incidentes**. Esto incluye la identificación de patrones como el aumento de **estrés en los trabajadores** o la frecuencia de pequeños incidentes que podrían preceder a accidentes mayores. Esta transformación **permite a las organizaciones implementar medidas correctivas** antes de que los riesgos se materialicen, optimizando recursos y protegiendo la integridad de los trabajadores.

Identificación predictiva de patrones de riesgo

Los sistemas de inteligencia artificial pueden analizar infinidad de variables de forma simultánea: condiciones ambientales, comportamientos de seguridad, historial de mantenimiento de equipos y factores humanos, entre otros.

Importancia de contar con una plataforma de software EHS

La seguridad, la salud y el cuidado del medio ambiente son pilares fundamentales en la sostenibilidad empresarial moderna. En este contexto, disponer de un Software EHS (Environment, Health and Safety) no es simplemente una herramienta tecnológica, sino un **requisito estratégico** para garantizar la eficiencia operativa, el cumplimiento normativo y la cultura preventiva dentro de las organizaciones.

El **Software EHS** se ha consolidado como un aliado indispensable para los responsables de **Seguridad y Salud en el Trabajo (SST)**, **Medio Ambiente**, y **Gestión del Riesgo**, facilitando la toma de decisiones informadas y promoviendo entornos laborales más seguros y sostenibles.

La evolución digital de la gestión EHS

Tradicionalmente, la gestión de la seguridad y la salud en el trabajo dependía de hojas de cálculo, formularios físicos y procesos manuales.

Sin embargo, la complejidad de las operaciones actuales —con múltiples sedes, normativas cambiantes y grandes volúmenes de datos— ha impulsado la **transformación digital de la gestión EHS**.

Un **Software EHS** centraliza toda la información relevante: indicadores, reportes, incidentes, auditorías, capacitaciones, matrices de riesgo y planes de acción. Este enfoque digital permite **integrar la prevención en tiempo real**, garantizando que los datos se actualicen de manera automática y se traduzcan en decisiones rápidas y efectivas.

Además, las plataformas modernas o soluciones líderes en el sector como **HSETools**, demuestran que la **personalización y accesibilidad** son claves en la nueva era de la gestión preventiva.

Los paneles de control personalizables, los accesos seguros y la posibilidad de escalar la gestión a nivel global hacen del software EHS una herramienta imprescindible para cualquier organización comprometida con la excelencia en seguridad.

Beneficios estratégicos de contar con un Software EHS

Implementar una plataforma de **Software EHS** aporta beneficios que van mucho más allá de la simple digitalización de procesos. Supone un **salto cualitativo** hacia la eficiencia, la trazabilidad y la sostenibilidad.

Observación del comportamiento en HSE: mejora de la seguridad y el rendimiento en el trabajo

Las observaciones de conducta juegan un papel esencial en la prevención de riesgos, ya que los accidentes laborales no siempre responden a fallos técnicos o equipos inadecuados. En ocasiones son comportamientos inseguros los que desencadenan incidentes graves. A pesar de contar con protocolos avanzados y equipos de protección, las organizaciones siguen registrando lesiones que podrían haberse evitado mediante la **observación del comportamiento** y la intervención temprana.

Esta realidad sobre la siniestralidad laboral evidencia que la tecnología y las normas, por sí solas, resultan insuficientes sin un enfoque que aborde el factor humano de forma sistemática. La observación del comportamiento es la respuesta a esta necesidad. **Se trata de un enfoque proactivo** que identifica, analiza y corrige acciones de riesgo antes de que deriven en accidentes. Al integrar

datos objetivos sobre el desempeño real de los trabajadores, las empresas pueden **diseñar intervenciones específicas, reforzar conductas seguras** y construir una **cultura de prevención** sólida. Así, la observación del comportamiento transforma la gestión de la seguridad de reactiva a proactiva y de punitiva a colaborativa.

Qué es la observación del comportamiento en HSE

La observación del comportamiento es un método estructurado que se centra en analizar las acciones de los empleados durante sus tareas habituales. **El objetivo no es fiscalizar, sino identificar patrones de riesgo y oportunidades de mejora** a través de datos objetivos. Este enfoque complementa las medidas tradicionales centradas en riesgos físicos o ambientales. Mientras que la prevención tradicional aborda instalaciones, maquinaria o condiciones del entorno, la observación del comportamiento se centra en el **factor humano**. Se trata de **comprender las causas de las acciones de los trabajadores** y facilitar alternativas más seguras. Un programa efectivo de observación del comportamiento **requiere observación sistemática, registro preciso, análisis de tendencias y comunicación bidireccional**. La participación activa de todos los niveles jerárquicos resulta fundamental para garantizar su éxito y sostenibilidad en el tiempo.

Principios clave de la observación del comportamiento

La implementación eficaz de un programa de observación del comportamiento se sustenta en **varios pilares estratégicos que aseguran su efectividad** y aceptación organizacional.

Evaluar el programa HSE: guía para una evaluación rigurosa y sistemática

Evaluar el programa HSE se ha convertido en una práctica indispensable para cualquier organización comprometida con la seguridad, la sostenibilidad y el cumplimiento normativo. En un entorno cada vez más regulado, no se trata solo de verificar que los procedimientos incluidos en los **programas HSE** se cumplen, sino de garantizar que los sistemas realmente funcionan, aportan valor y se adaptan a los nuevos desafíos legales y operativos.

Las organizaciones que no realizan estas evaluaciones periódicas corren el riesgo de operar con información desactualizada, procesos ineficientes o estrategias que no responden al contexto de cada momento. **Una evaluación rigurosa permite identificar carencias y cuantificar resultados**, aspectos esenciales para la mejora continua del desempeño en materia de seguridad, salud y medio ambiente.

Beneficios clave de evaluar el programa HSE

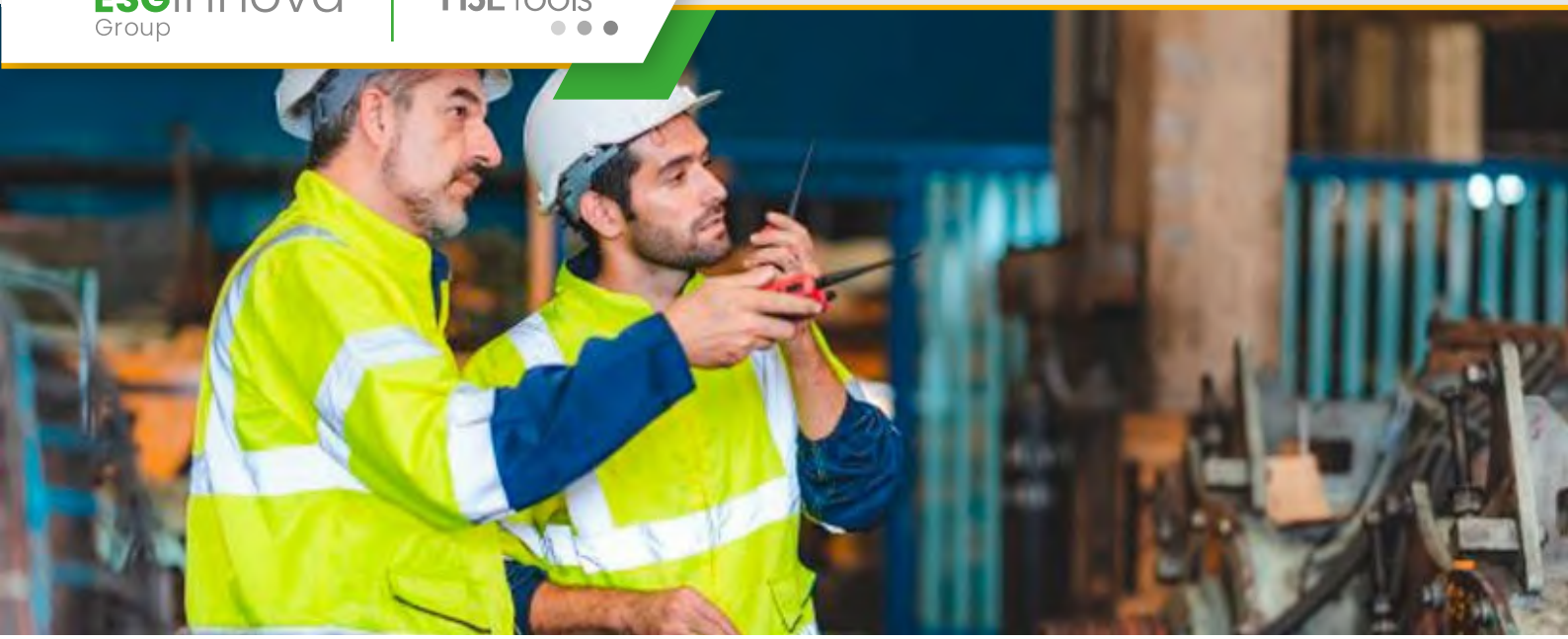
Evaluar el programa HSE de una organización ofrece **beneficios a corto y largo plazo**, pero hay tres de especial relevancia:

Hace visible el éxito y demuestra resultados

Uno de los retos de los responsables HSE es demostrar el valor tangible de sus programas ante la alta dirección. Mientras que los accidentes, incidentes o sanciones evidencian fallos, los logros en la **gestión de prevención de riesgos** suelen pasar inadvertidos. Evaluar el programa HSE de forma estructurada **permite traducir la seguridad y la sostenibilidad en datos verificables**: reducción de incidentes, mejoras de productividad o ahorro en primas de seguros. Estos indicadores objetivos son esenciales para justificar inversiones, optimizar recursos y consolidar una cultura organizacional que **perciba la gestión HSE no como un coste, sino como una inversión estratégica**.

Alinea el programa con los cambios normativos y organizativos

Las normativas evolucionan de forma constante, al igual que los requisitos de estándares como **ISO 45001** o ISO 14001. **Evaluar el programa HSE ayuda a detectar desviaciones** y verificar que las políticas, procedimientos y registros continúan alineados con los estándares aplicables, evitando así sanciones o no conformidades. No solo las normas, también las organizaciones cambian. La incorporación de nuevos procesos, tecnologías o plantillas modifica las condiciones de riesgo y una evaluación periódica **garantiza que el sistema evoluciona al mismo ritmo que la empresa**, evitando que quede obsoleto.



Herramientas y técnicas para observaciones de seguridad eficaces

Las observaciones de seguridad son una de las herramientas más poderosas para prevenir accidentes laborales y fortalecer la cultura preventiva en las organizaciones. Sin embargo, su verdadero valor está en convertirlas en información útil, sistematizada y capaz de impulsar la mejora continua. Las **observaciones de conducta** en seguridad laboral permiten identificar patrones de riesgo, reforzar comportamientos seguros y transformar la seguridad en un proceso de aprendizaje constante.

En un entorno donde la automatización y la digitalización avanzan con rapidez, las observaciones de seguridad se han consolidado como un componente estratégico dentro de los **sistemas de gestión HSE**. Gracias a la tecnología, **las empresas pueden evolucionar desde un enfoque reactivo hacia uno predictivo** donde el análisis de datos y la inteligencia artificial anticipan los riesgos antes de que ocurran.

La importancia de estructurar las observaciones de seguridad

Un programa de observaciones de seguridad eficaz comienza por definir un marco metodológico claro. **Sin una estructura, los datos recogidos pierden coherencia** y la información no se transforma en acción. Entre sus pilares destacan:

Definir objetivos claros

Toda observación debe tener un propósito: identificar comportamientos inseguros, medir la efectividad de los controles o evaluar el grado de cumplimiento de las normas internas. Establecer objetivos específicos y medibles **ayuda a orientar los esfuerzos y medir el impacto de las acciones**.

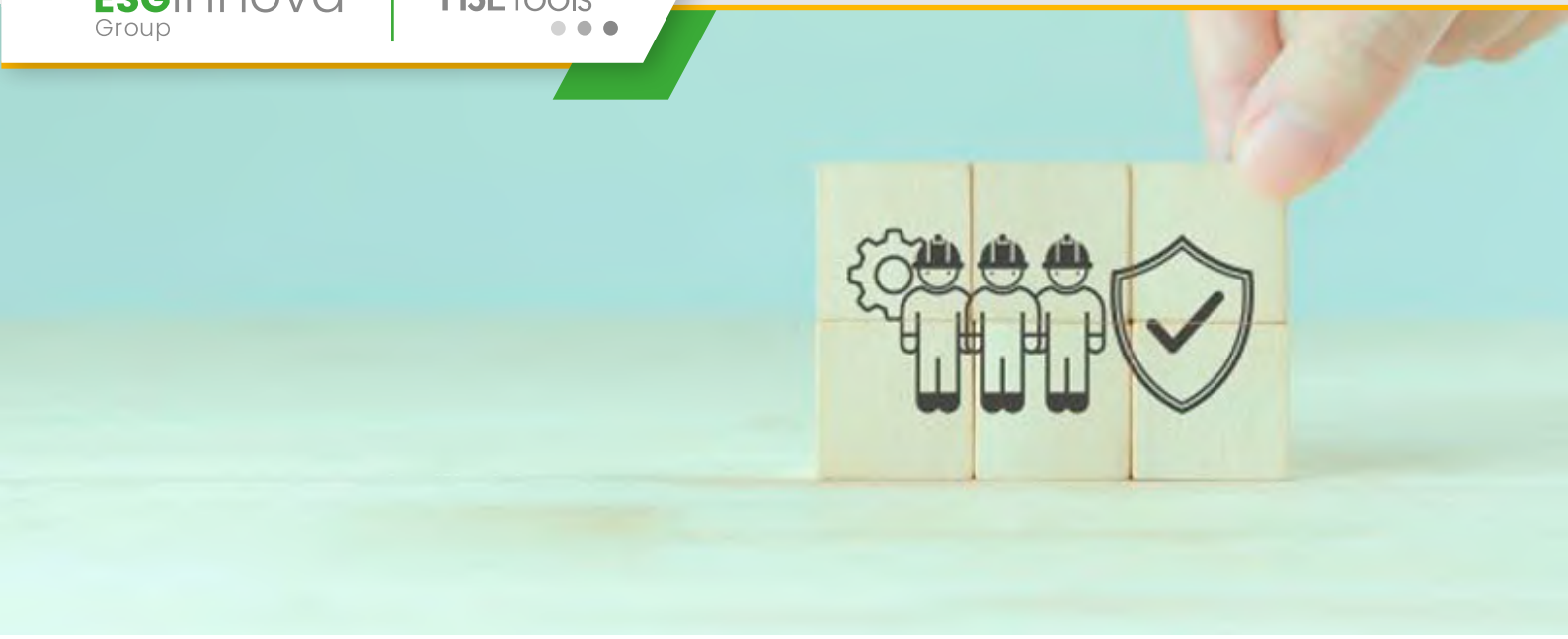
Listas de verificación estandarizadas

Garantizan que los observadores sigan criterios homogéneos y no pasen por alto aspectos relevantes. Una lista bien diseñada cubre tanto conductas como condiciones críticas de seguridad. Digitalizar estas listas permite mayor trazabilidad y facilita su análisis posterior. La coherencia en las observaciones aumenta la fiabilidad de los datos y, por tanto, la capacidad de mejora.

Capacitación y liderazgo: pilares de la observación eficaz

El observador es, en realidad, un agente de cambio. Su formación no debe centrarse solo en identificar comportamientos, sino también en desarrollar una **comunicación eficaz** con los trabajadores y ofrecer una retroalimentación constructiva.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Software HSE para empresas: cómo fortalecer tu cultura de seguridad

Toda organización posee su propia cultura corporativa, pero dentro de ella existe un elemento fundamental: la cultura de seguridad. Este concepto es mucho más que un conjunto de normativas y protocolos, representa el compromiso compartido de todos los niveles jerárquicos hacia la protección de las personas, el medio ambiente y los activos empresariales. Un software HSE para empresas es una herramienta básica para consolidar esa estrategia, en la que la **gestión de la documentación** es clave.

Las soluciones digitales de gestión HSE permiten integrar la información, estandarizar procesos y reforzar comportamientos seguros en todos los niveles de la organización. Así, la tecnología deja de ser un apoyo puntual para convertirse en el eje que **articula la prevención, la formación y la mejora continua de la seguridad laboral**.

La cultura de seguridad: una responsabilidad compartida

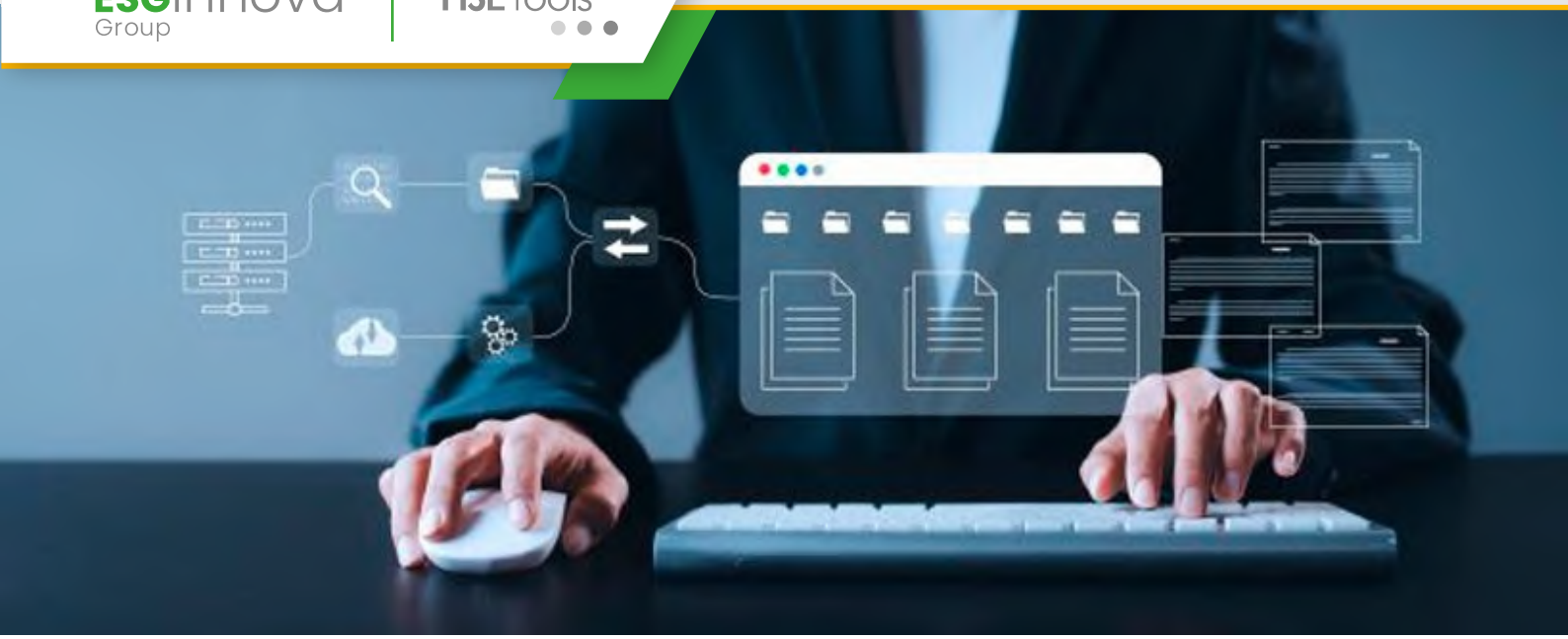
La **cultura de seguridad** se define como el **conjunto de valores, actitudes y prácticas** que determinan el compromiso real de una empresa con la protección de las personas y el entorno. No surge de forma espontánea, sino que requiere coherencia entre la estrategia, la comunicación y los recursos disponibles. Directivos y mandos intermedios desempeñan un papel clave. Sin embargo, el verdadero cambio se consolida cuando la cultura se integra en todos los niveles jerárquicos y cada empleado entiende su papel dentro del sistema preventivo. Para ello, la **transformación digital en la gestión HSE** es indispensable: **permite comunicar objetivos, supervisar resultados y fomentar la participación activa de los trabajadores** en la mejora de la seguridad.

Cómo el software HSE para empresas impulsa la seguridad organizacional

El software HSE para empresas actúa como la base tecnológica sobre la que se construye una cultura de seguridad sólida. **Centraliza datos, automatiza procesos y genera indicadores que permiten a las organizaciones anticiparse al riesgo**. Pero, sobre todo, impulsa la responsabilidad compartida, convirtiendo la seguridad en un elemento operativo y medible, no en una simple declaración de intenciones.

Identificación y gestión de riesgos en tiempo real

La prevención empieza con el conocimiento. Un software HSE para empresas integra herramientas que permiten identificar peligros, evaluar su probabilidad e impacto y priorizar acciones correctivas.



Software para inspecciones de seguridad: del papel a la prevención inteligente de incidentes

En un entorno laboral dinámico y exigente, las **inspecciones y checklist** de seguridad no pueden depender de formularios en papel ni de procesos manuales. Las organizaciones que buscan eficiencia, cumplimiento normativo y prevención efectiva necesitan soluciones digitales que transformen la forma en que gestionan sus riesgos. El **software para inspecciones de seguridad** permite modernizar la gestión HSE, ayudando a los equipos a actuar con rapidez, precisión y visión preventiva.

Desde la trazabilidad de hallazgos hasta la automatización de acciones correctivas, el software para inspecciones de seguridad **permite a las empresas anticiparse a los incidentes, optimizar recursos y fortalecer su cultura preventiva**.

Software para inspecciones de seguridad: una herramienta activa

Durante mucho tiempo, las listas de verificación en papel han sido el estándar para realizar **inspecciones de seguridad**. Aunque cumplían funciones básicas como verificar el estado de equipos o condiciones laborales, su utilidad es limitada. **Las listas en papel son fáciles de extraviar, lentas de procesar y no ofrecen capacidad de respuesta inmediata**. Un hallazgo crítico puede quedar sin respuesta durante horas, comprometiendo la seguridad operativa. Además, **la falta de trazabilidad dificulta la implementación de acciones correctivas** y el seguimiento de los compromisos adquiridos. En contextos donde el tiempo es un factor decisivo, esta lentitud puede traducirse en incidentes evitables.

El paso hacia la digitalización

La **transformación digital** significa un avance decisivo hacia una gestión SST inteligente y proactiva. El uso de tabletas, aplicaciones móviles y plataformas en la nube permite **capturar datos sobre el terreno y compartirlos en tiempo real** con los responsables. Sin embargo, las soluciones iniciales replicaban el modelo estático del papel: formularios digitales que no reaccionaban ante las respuestas ni ofrecían orientación contextual.

Por eso, para que la digitalización aporte verdadero valor, debe ir más allá de la simple captura de datos. Debe convertirse en **una herramienta activa que guíe decisiones, priorice riesgos y facilite la acción inmediata**.

Seguridad y salud de contratistas: cómo crear un programa que funcione

La **seguridad y salud de contratistas** es un aspecto crítico, especialmente en sectores como la construcción, la industria pesada o la energía. Las organizaciones que externalizan tareas deben garantizar que esos trabajadores operen bajo los mismos estándares de seguridad que el personal interno. Para ello, son necesarios programas de **gestión de contratistas** sólidos, estructurados y adaptables a múltiples entornos operativos.

En un contexto marcado por la presión normativa, la digitalización de procesos y la creciente complejidad de los proyectos, las empresas necesitan soluciones eficaces para gestionar la seguridad de la fuerza laboral externa. Un programa bien diseñado no solo reduce riesgos legales y operativos, sino que también **refuerza la cultura preventiva, mejora la reputación corporativa y optimiza el rendimiento global**.

Definición y alcance de la gestión de seguridad y salud de contratistas

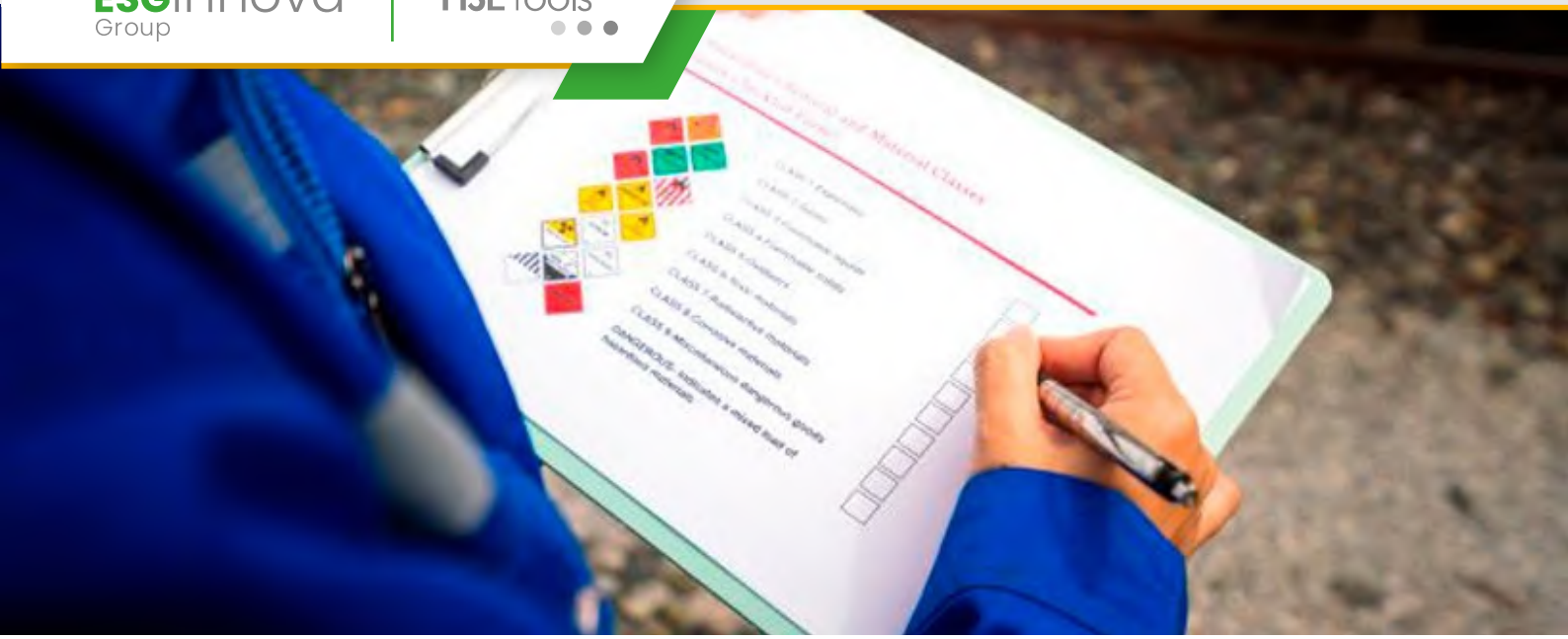
La gestión de seguridad y salud de contratistas constituye un proceso sistemático que **asegura el cumplimiento de todas las normas y prácticas de seguridad** requeridas. Este sistema protege a los trabajadores, previene incidentes y garantiza el cumplimiento normativo mediante la integración de múltiples elementos coordinados. **Un programa robusto incluye la precalificación basada en historial de seguridad**, **capacitación de seguridad** adaptada a riesgos específicos del sitio, supervisión continua durante el trabajo, y análisis posterior de incidentes para prevenir recurrencias.

Responsabilidad compartida

Los contratistas deben proteger a sus empleados proporcionándoles formación adecuada, **equipos de protección personal** y supervisión competente. Simultáneamente, la organización contratante debe garantizar el cumplimiento de políticas de seguridad corporativas y obligaciones legales. Esta responsabilidad compartida **asegura protección para todos los trabajadores**.

Marco normativo aplicable

La gestión se rige por normativas nacionales e internacionales. ISO 45001 representa el estándar global para Sistemas de Gestión de Seguridad y Salud Ocupacional. Mientras, directivas europeas y legislaciones de los estados establecen requisitos específicos para la coordinación de actividades empresariales. Todo ello se debe tener en cuenta.



Programas de salud y seguridad: 8 errores comunes y cómo solucionarlos

Los **programas de salud y seguridad** son el eje de cualquier estrategia empresarial responsable. No solo protegen el bienestar de los empleados, sino que contribuyen de forma decisiva a la continuidad operativa y al cumplimiento normativo. Todo ello sin olvidar su papel en la reputación de la organización. Sin embargo, incluso los **programas HSE** mejor diseñados pueden fracasar si la gestión se apoya en procedimientos desactualizados, una comunicación deficiente o no hay una integración tecnológica.

En un entorno donde las normativas evolucionan rápidamente y la digitalización redefine la gestión del riesgo, **los errores más comunes en los programas de salud y seguridad no derivan de la falta de compromiso, sino de una gestión poco estructurada**. A continuación, se analizan los fallos más habituales, su impacto en la eficacia del sistema y cómo la tecnología puede convertirse en el mejor aliado para una **cultura preventiva** sólida.

1. Riesgos mal identificados: origen de accidentes

Todo sistema eficaz parte de una **evaluación de riesgos** rigurosa y continua. Cuando la organización no identifica los peligros reales (físicos, químicos, ergonómicos o psicosociales), el programa pierde consistencia.

La falta de documentación, el exceso de confianza o la dependencia de evaluaciones puntuales son errores frecuentes. Los programas de salud y seguridad más avanzados se apoyan en un **software HSE** que integre la identificación automática de riesgos, permita registrar observaciones en campo y analizar tendencias mediante IA. Con ello, **la empresa pasa de una gestión reactiva a una prevención proactiva y basada en datos**, minimizando la probabilidad de incidentes.

2. Falta de análisis de incidentes leves: error común en programas de salud y seguridad

Un incidente sin consecuencias graves puede ser el aviso de un problema mayor. **No analizarlo implica perder información crítica**. La falta de un procedimiento de reporte digitalizado o de seguimiento sistemático suele derivar en repetición de errores.

La tecnología permite capturar estos eventos en tiempo real, incluso desde dispositivos móviles, y generar alertas automáticas para que el responsable evalúe causas raíz y adopte medidas correctivas. Esta práctica en los programas de salud y seguridad refuerza la mejora continua, principio esencial de la norma **ISO 45001**.

KPI de seguridad: indicadores adelantados y rezagados clave para las empresas

Seguridad salud son pilares fundamentales en los **programas HSE** de las organizaciones. Establecer **KPI de seguridad** (indicador clave de rendimiento) robusto es la referencia esencial en la gestión. Sin métricas claras, la toma de decisiones se reduce a conjeturas, impidiendo identificar riesgos o medir el impacto de las mejoras adoptadas.

El desafío para los responsables de HSE es qué medir y cómo usar esa información. Muchas organizaciones se anclan en métricas obsoletas, reaccionando a los accidentes en lugar de prevenirlos. **La transformación digital ofrece la oportunidad de pasar de una visión reactiva a una gestión proactiva y predictiva**.

Qué es un KPI de seguridad y por qué es tan importante

Un KPI de seguridad, en el ámbito de HSE, es un valor medible que evalúa la eficacia con la que una organización alcanza sus objetivos

específicos de seguridad. Estos indicadores **proporcionan un marco claro para identificar tendencias** y realizar un seguimiento del progreso.

Beneficios definir y monitorizar KPI de seguridad

Definir y supervisar los KPI de seguridad **aporta estructura, claridad y dirección a todo el programa HSE**. Cuando los **indicadores de gestión SST** están bien definidos, se convierten en la base para una toma de decisiones proactiva. Entre los beneficios cabe destacar los siguientes:

- **Identificación temprana de riesgos**: permiten identificar peligros potenciales con antelación.
- **Asignación eficaz de recursos**: ayudan a decidir dónde invertir tiempo y dinero para alcanzar un mayor impacto.
- **Comparativas**: facilitan la comparación del **desempeño del programa SST** entre diferentes centros de trabajo o períodos.
- **Fomento de la credibilidad**: demostrar un progreso cuantificable genera confianza en la alta dirección.

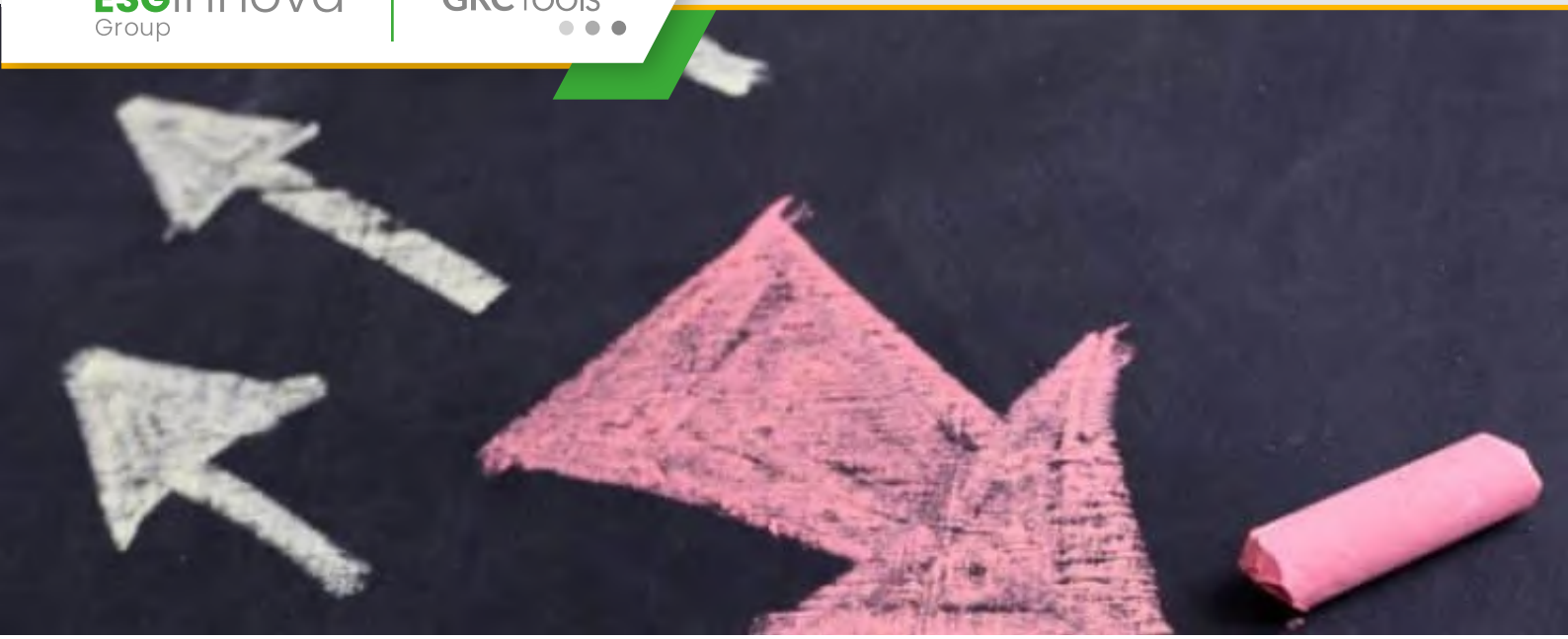
Indicadores adelantados vs. indicadores rezagados

Para una visión completa, **es indispensable seguir tanto indicadores adelantados como rezagados**. Basarse solo en un tipo de KPI de seguridad ofrece una imagen sesgada. Los adelantados ayudan a anticipar riesgos, mientras que los rezagados ayudan a aprender de los sucesos pasados.

ESGinnova Group

GRCTools

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



¿Cómo tomar decisiones estratégicas en base a la gestión de riesgos?

El mundo empresarial actual se define por la incertidumbre, la presión de los mercados globales y el impacto de la disrupción tecnológica. Frente a este panorama, las organizaciones afrontan un mismo desafío: **cómo tomar decisiones estratégicas** que no solo impulsen el crecimiento, sino que también aseguren la sostenibilidad y la resiliencia. En este contexto, la **gestión de riesgos** deja de ser una actividad meramente preventiva para convertirse en un habilitador clave de la estrategia.

Dos marcos de referencia reconocidos a nivel internacional destacan en esta materia. Por un lado, la **ISO 31000**, que ofrece principios y directrices adaptables a cualquier organización, independientemente de su tamaño o sector. Por otro, el **COSO ERM**, que pone el foco en integrar la gestión de riesgos con la estrategia y el desempeño, aportando un enfoque orientado al valor y la gobernanza.

Ambos coinciden en un mensaje central: las **decisiones estratégicas** más sólidas son aquellas que se fundamentan en una comprensión profunda de los riesgos y oportunidades que rodean al negocio.

La gestión de riesgos como motor de decisiones estratégicas

Lejos de limitarse a evitar pérdidas, la gestión de riesgos estratégica ayuda a las organizaciones a identificar oportunidades, fortalecer su resiliencia y crear un marco de referencia más realista para el futuro. Integrar esta práctica en la dirección corporativa ofrece beneficios tangibles:

- **Anticipación de amenazas y oportunidades**: permite prever escenarios que podrían afectar negativamente y, al mismo tiempo, identificar ventajas competitivas.
- **Mejor planificación estratégica**: al integrar evaluaciones de riesgo en la planificación, se construyen hojas de ruta más ajustadas a la realidad.
- **Fortalecimiento de la resiliencia organizacional**: contar con un sistema de riesgos robusto prepara a la empresa frente a cambios regulatorios, tecnológicos o sociales.
- **Alineación del riesgo con los objetivos**: algunas decisiones estratégicas implican aceptar riesgos controlados cuando estos están vinculados a innovación o crecimiento.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo llevar a cabo una gestión proactiva de los riesgos de terceros

En la actualidad, ninguna organización puede considerarse una isla. Cada empresa forma parte de un entramado de **proveedores, contratistas, distribuidores, socios estratégicos y prestadores de servicios** que sostienen su funcionamiento diario. Esta red interdependiente potencia la innovación y la eficiencia, pero también abre la puerta a **riesgos de cumplimiento, operacionales, financieros y reputacionales** que pueden comprometer la continuidad del negocio.

Por ello, implementar una **gestión proactiva de los riesgos de terceros** se ha convertido en un **imperativo estratégico**. Ya no basta con evaluar a los proveedores una vez al año o revisar sus certificaciones: las organizaciones necesitan un **modelo de gobernanza integral**, sustentado en tecnología y alineado con sus objetivos corporativos.

Más allá del control: la gobernanza de terceros como ventaja competitiva

Tradicionalmente, el enfoque de **Third-Party Risk Management (TPRM)** se limitaba a los procesos de contratación y evaluación de proveedores. Sin embargo, en el entorno actual, este enfoque resulta insuficiente. Las organizaciones líderes están adoptando una **visión holística de Gobernanza, Riesgo y Cumplimiento (GRC)**, que abarca todo el **ciclo de vida del tercero**: desde la **incorporación (onboarding)** y la **supervisión continua**, hasta la **desvinculación (offboarding)**.

Una **gestión proactiva de los riesgos de terceros** implica actuar antes de que los incidentes ocurran, identificando vulnerabilidades, midiendo su impacto y asegurando que cada relación con un tercero aporte valor y no exposición. Para lograrlo, las empresas deben:

- **Centralizar la información de riesgo de terceros**, creando una visión unificada del ecosistema.
- **Aplicar una debida diligencia continua**, no solo inicial.
- **Monitorear en tiempo real el desempeño y el cumplimiento** de los proveedores.
- **Alinear las obligaciones contractuales con los requisitos regulatorios**.
- **Automatizar los flujos de trabajo** para la incorporación, seguimiento y remediación de incidentes.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Qué es el modelo Cuatro Líneas de Defensa en la gestión de riesgo empresarial

La adecuada **gestión de los riesgos empresariales** requiere no solo identificar y medir los posibles eventos adversos, sino también establecer una estructura clara de funciones, controles y responsabilidades. En este sentido, el **modelo Cuatro Líneas de Defensa** se ha convertido en una herramienta clave para reforzar la gobernanza, el control interno y la supervisión organizacional.

El modelo tradicional de las tres líneas de defensa ha sido ampliamente adoptado en empresas e instituciones. Sin embargo, con el auge de la función de **cumplimiento normativo (Compliance)** y la complejidad creciente del entorno regulatorio, muchas organizaciones han evolucionado hacia una versión ampliada: el modelo cuatro líneas.

A continuación, examinaremos en detalle qué es, por qué es útil, cómo se despliega en la práctica y qué beneficios aporta al riesgo corporativo.

¿En qué consiste el modelo Cuatro Líneas de Defensa?

El modelo Cuatro Líneas de Defensa propone que la gestión y control de riesgos se organice en **cuatro capas o niveles diferenciados**, cada una con funciones específicas, responsabilidad y grado de independencia.

Línea 1 – Gestión operativa

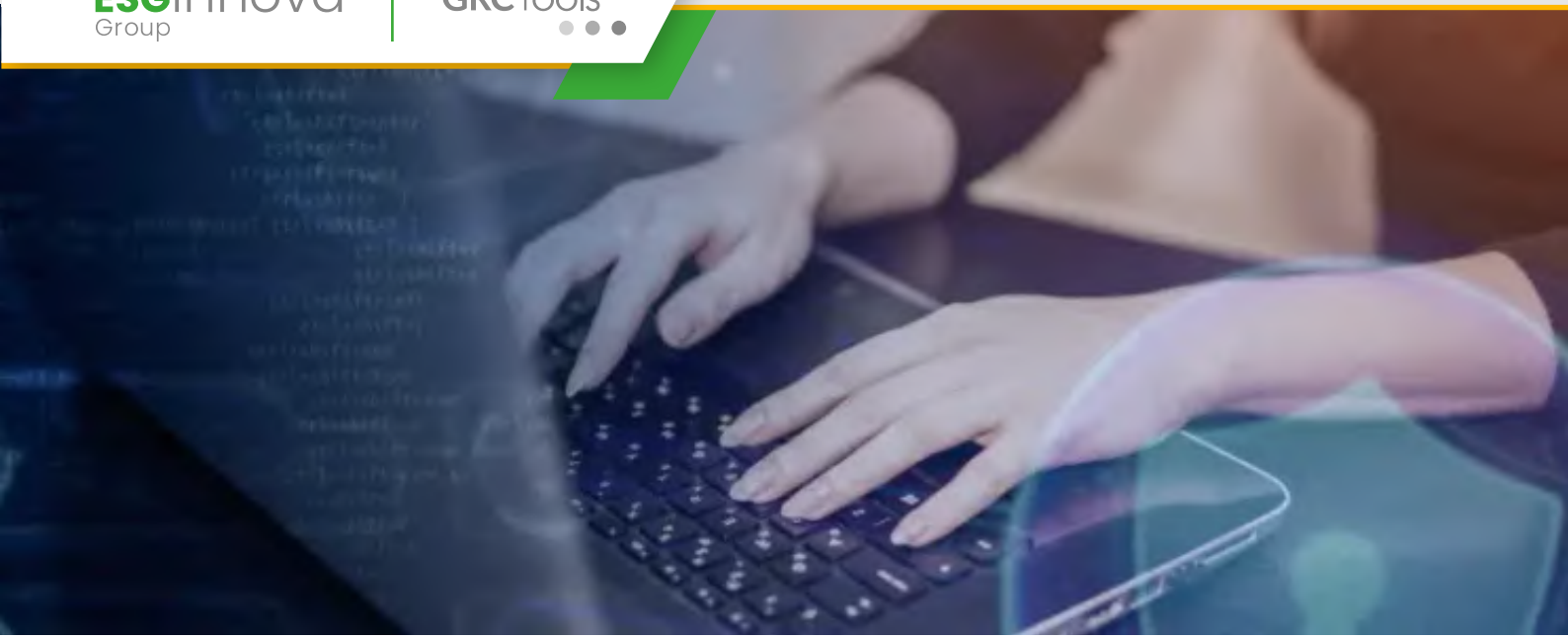
La primera línea está compuesta por las unidades de negocio, los gerentes de proceso y los equipos operativos, quienes son **propietarios directos de los riesgos**. Ellos deben identificar, medir, controlar y mitigar los riesgos inherentes a sus actividades diarias. Se encargan del diseño y ejecución de los controles internos, del cumplimiento básico de políticas y procedimientos, y de la gestión de los eventos que puedan materializarse.

Línea 2 – Supervisión de riesgos y control interno

La segunda línea agrupa funciones como gestión de riesgos, control interno, contraloría o auditoría de procesos internos de supervisión. Su función es diseñar marcos de control, metodologías de riesgos, indicadores clave, además de **asesorar y supervisar** a la primera línea para asegurar que operen dentro del apetito de riesgo definido.

Línea 3 – Cumplimiento normativo (Compliance)

En el modelo expandido de cuatro líneas, la función de **Compliance** se sitúa como tercera línea de defensa independiente. El Compliance Officer vela por que la organización cumpla con leyes, regulaciones, estándares éticos y políticas internas.



¿Cómo cumplir eficazmente con NIS 2?

La **Directiva NIS 2** marca un antes y un después en la **ciberseguridad europea**. Su entrada en vigor amplía el alcance de la antigua NIS (Network and Information Security Directive) y establece **nuevas obligaciones legales, técnicas y de gobernanza** para garantizar la **resiliencia digital** de las organizaciones que operan dentro de la Unión Europea.

No obstante, cumplir con NIS 2 no se limita a redactar políticas o acumular documentación: requiere **acciones concretas**, coordinación entre áreas y un enfoque integral de **gobierno, riesgo y cumplimiento (GRC)**. En este artículo te explicamos qué exige la NIS 2, cuáles son sus desafíos y cómo implementar un cumplimiento realmente eficaz.

¿Qué es la Directiva NIS 2?

La **Directiva (UE) 2022/2555**, conocida como **NIS 2**, fue aprobada por el Parlamento Europeo y el Consejo en diciembre de 2022 y debió ser transpuesta por los Estados miembros antes de octubre

de 2024. Su objetivo es **reforzar la ciberresiliencia** de los sectores esenciales y de los servicios digitales críticos en toda la Unión Europea.

A diferencia de la primera directiva NIS (2016), NIS 2 amplía su alcance, endurece las sanciones y otorga **mayor responsabilidad a la alta dirección** en materia de seguridad y cumplimiento.

Entre sus principales novedades destacan:

- **Ampliación del ámbito de aplicación**: incluye más sectores —energía, transporte, salud, gestión de residuos, administración pública, servicios digitales, entre otros— y categorías de entidades "esenciales" e "importantes".

- **Responsabilidad de la alta dirección**: los directivos deben aprobar las políticas de ciberseguridad, supervisar su ejecución y pueden ser sancionados personalmente por incumplimiento.

- **Requisitos de gestión de riesgos y medidas técnicas**: las organizaciones deben establecer políticas de control de acceso, gestión de incidentes, continuidad operativa y seguridad de la cadena de suministro.

- **Obligación de notificar incidentes**: las entidades afectadas deben reportar incidentes significativos en un plazo máximo de 24 horas.

- **Sanciones más severas**: multas que pueden alcanzar hasta el 2 % del volumen de negocio global anual o 10 millones de euros, dependiendo del tipo de organización.

Retorno de la inversión (ROI): elemento esencial en la gestión de riesgos

En el mundo empresarial actual, la **gestión de riesgos** se ha convertido en un pilar fundamental para la sostenibilidad, la rentabilidad y la resiliencia organizacional. Las empresas ya no pueden limitarse a identificar amenazas y asignar matrices de riesgo; ahora deben evaluar **cuánto valor genera cada decisión** tomada para mitigar o aceptar un riesgo.

Aquí es donde entra en juego un concepto clave que, aunque a veces olvidado, resulta determinante: el **Retorno de la Inversión (ROI)**. Entender el ROI dentro de la gestión de riesgos significa medir la **efectividad económica de las acciones preventivas y correctivas**, permitiendo que las decisiones de mitigación sean más racionales, competitivas y alineadas con los objetivos estratégicos del negocio.

Por qué el ROI debe formar parte de la gestión de riesgos

Durante años, los programas de **gestión de riesgos** han estado dominados por enfoques técnicos y metodológicos centrados en identificar, evaluar y reportar amenazas. Sin embargo, esta visión se queda corta si no se acompaña de una pregunta crítica: **¿qué valor obtiene la organización al invertir en reducir un riesgo?**

Cada acción de mitigación —ya sea un nuevo control interno, una mejora tecnológica o un plan de contingencia— implica un **costo**. Y, en un entorno donde los recursos financieros y humanos son limitados, las empresas deben asegurarse de que **cada euro invertido aporte un beneficio tangible**.

El ROI aporta esa perspectiva cuantitativa que permite **comparar diferentes tratamientos de riesgo**, priorizar inversiones y justificar decisiones ante la alta dirección o los accionistas. En otras palabras, convierte la gestión de riesgos en un proceso **estratégico y medible**, no en un simple ejercicio de cumplimiento.

Riesgos que compiten por recursos: el dilema del capital limitado

En toda organización, los recursos económicos son finitos. Los proyectos de mitigación deben competir con otras prioridades como innovación, sostenibilidad o transformación digital.

Por tanto, cada acción dentro del plan de gestión de riesgos —instalar una nueva herramienta, capacitar equipos, reforzar ciberseguridad, contratar seguros— debe ser tratada como una **decisión de inversión**, sujeta a criterios de rentabilidad.

Directiva de ciberseguridad de la UE NIS2

La **Directiva de ciberseguridad de la UE NIS2** marca un antes y un después en la forma en que las organizaciones europeas deben abordar la seguridad de la información. Nacida como una evolución de la Directiva NIS de 2016, esta nueva regulación refuerza los requisitos de ciberseguridad, amplía su alcance y eleva la responsabilidad de la alta dirección. Su objetivo es claro: **garantizar un nivel común de resiliencia digital en toda la Unión Europea** frente a un entorno cada vez más amenazado por ciberataques, interrupciones de servicio y vulnerabilidades tecnológicas.

Directiva de ciberseguridad de la UE NIS2: un marco común para una Europa más cibersegura

La **Directiva NIS2 (Directiva UE 2022/2555)** fue aprobada por el Parlamento Europeo y el Consejo en diciembre de 2022 y debió ser transpuesta por todos los Estados miembros antes del 17 de octubre de 2024. Su propósito es unificar los estándares de ciberseguridad en los diferentes países europeos, evitando la fragmentación normativa que se observó tras la primera directiva NIS.

A diferencia de su predecesora, la NIS2 **amplía el número de sectores y organizaciones obligadas a cumplir con sus disposiciones**, incluyendo operadores de servicios esenciales, proveedores de servicios digitales, administraciones públicas y entidades críticas de infraestructuras tecnológicas. Además, la directiva tiene un **alcance extraterritorial**, aplicándose también a empresas fuera de la UE que presten servicios relevantes al mercado europeo.

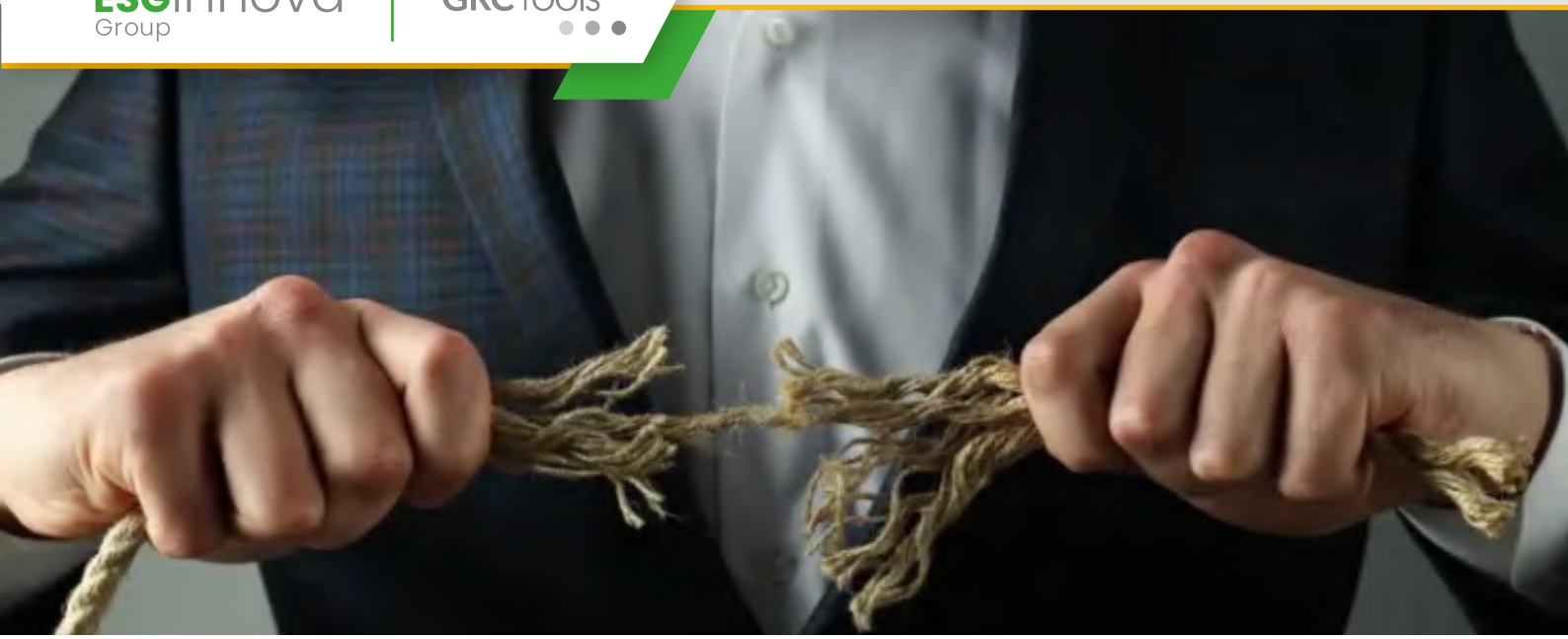
En España, su supervisión recaerá en las autoridades competentes de cada sector, con apoyo del **Centro Criptológico Nacional (CCN)** y del **Instituto Nacional de Ciberseguridad (INCIBE)**.

Propósito y alcance de la Directiva NIS2

El principal objetivo de la **Directiva de ciberseguridad de la UE NIS2** es fortalecer la **resiliencia digital y la capacidad de respuesta** de las organizaciones europeas. Con un enfoque preventivo y estratégico, busca reducir los riesgos derivados de ciberincidentes mediante la adopción de medidas técnicas, organizativas y de gobernanza.

Su propósito abarca tanto la **protección de infraestructuras críticas** como la **armonización de las normativas nacionales**, creando un marco común que fomente la cooperación transfronteriza entre los Estados miembros.

En consecuencia, la ciberseguridad deja de ser una función técnica aislada para convertirse en una **responsabilidad corporativa**, supervisada directamente por la alta dirección.



Preparación ante emergencias y riesgos de interrupción del negocio

En un contexto global cada vez más volátil, las organizaciones enfrentan una amenaza constante: los riesgos de **interrupción del negocio**. Desde desastres naturales hasta ciberataques, fallas tecnológicas o emergencias médicas, los eventos disruptivos pueden detener operaciones críticas en cuestión de minutos. La clave para sobrevivir no es evitar lo inevitable, sino **prepararse estratégicamente para afrontarlo**.

La **preparación ante emergencias** ya no se limita a cumplir con requisitos normativos o a instalar equipamiento básico, como un desfibrilador automático externo (DEA). Implica adoptar un enfoque integral de **gestión de continuidad**, capaz de proteger a las personas, los activos, los datos y la reputación corporativa. Un plan sólido no solo salva vidas, también que **reduce los riesgos de interrupción del negocio**, acelera la recuperación y fortalece la resiliencia organizacional.

La conexión entre emergencias y continuidad operativa

Los **riesgos de interrupción del negocio** son el resultado directo de una falta de preparación frente a eventos imprevistos. Una emergencia médica, un incendio, una falla eléctrica o un ataque cibernético pueden paralizar procesos esenciales, interrumpir la cadena de suministro o generar pérdidas económicas y de confianza irreversibles.

Por ello, la gestión de la **preparación ante emergencias** debe integrarse con los planes de **continuidad de negocio** y **gestión de riesgos corporativos**. Esta visión holística permite que la organización responda de manera coordinada y eficiente, garantizando la **operatividad mínima aceptable** mientras se restablecen las condiciones normales.

Las estadísticas son claras: en Estados Unidos, se registran cada año más de **356.000 paros cardíacos extrahospitalarios**, con una **tasa de mortalidad cercana al 90%** sin intervención inmediata. Cuando la respuesta es rápida y eficaz —mediante **RCP y uso de DEA**— la supervivencia puede alcanzar el **90%**, pero **disminuye un 10% por cada minuto de demora**. Esta misma lógica aplica al mundo empresarial: **cada minuto de inacción frente a una crisis aumenta exponencialmente el impacto financiero y operativo**.

Pilares de un programa de preparación ante emergencias

De acuerdo con las mejores prácticas internacionales y la experiencia de expertos como Timothy Papenfuss, de RescueStat, un programa de emergencia efectivo debe contemplar varios pilares esenciales.

5 consejos para reducir y evitar los riesgos financieros en la empresa

En el entorno empresarial actual, las compañías operan en un contexto lleno de incertidumbres y variables económicas que pueden afectar su estabilidad. Los **riesgos financieros en la empresa** constituyen una de las amenazas más relevantes: su manifestación puede comprometer la liquidez, la solvencia y la capacidad de inversión del negocio. Para una gestión eficaz, es imprescindible que los directivos comprendan qué implican esos riesgos, identifiquen sus fuentes y actúen de forma proactiva. A continuación, se presentan cinco consejos clave para **reducir y evitar los riesgos financieros** en la empresa, con un enfoque profesional y operativo.

¿Qué son los riesgos financieros en la empresa?

El término **riesgo financiero** hace referencia a la probabilidad de que una empresa sufra pérdidas económicas o no obtenga los resultados esperados debido a factores internos o externos vinculados con las finanzas.

Para una empresa, estos riesgos pueden emerger por cambios en los mercados, falta de liquidez, incumplimientos de clientes, variaciones de tipo de cambio o fallos operativos en la gestión financiera.

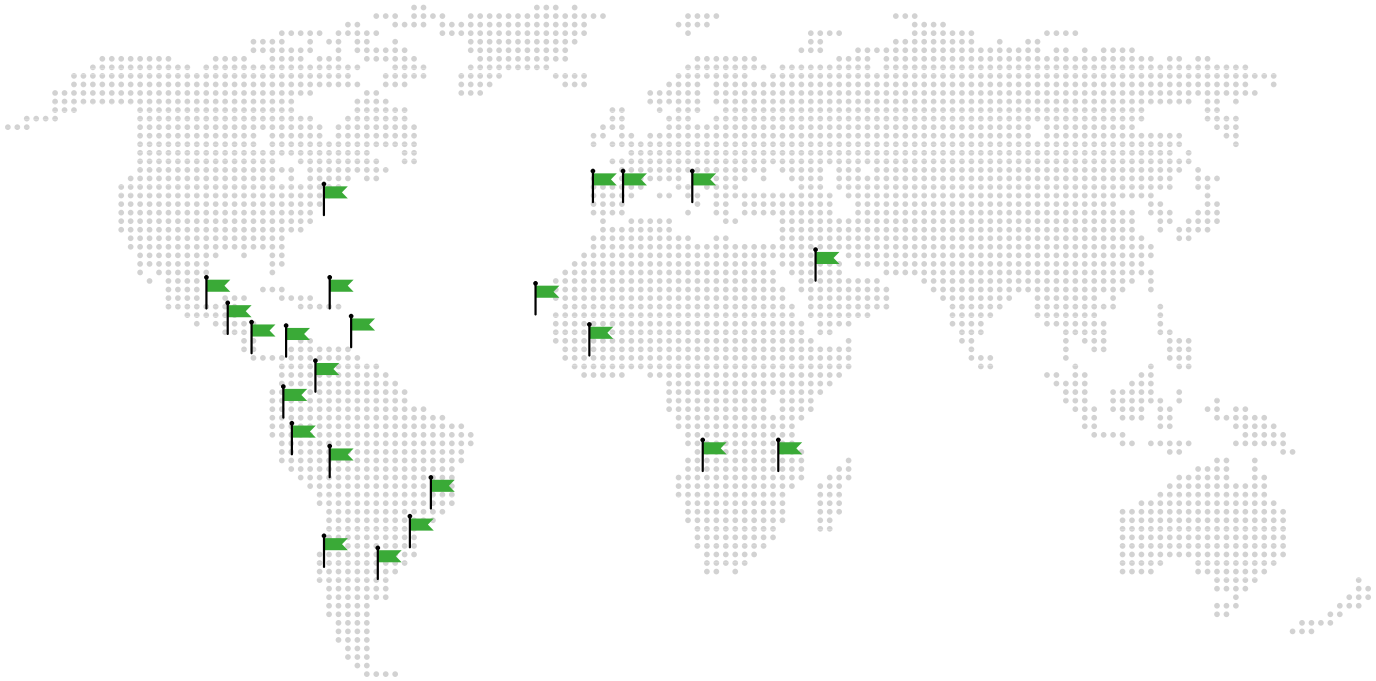
Identificar y gestionar correctamente los riesgos financieros en la empresa permite reforzar la resiliencia, mantener la credibilidad frente a los grupos de interés y asegurar la continuidad del negocio.

Tipos más comunes de riesgos financieros

Algunos de los principales tipos de riesgos que afectan a las empresas son:

- **Riesgo de mercado**: vinculado con fluctuaciones en precios, tasas de interés o tipos de cambio.
- **Riesgo de crédito**: cuando los clientes o deudores no cumplen sus obligaciones con la empresa.
- **Riesgo de liquidez**: incapacidad para hacer frente a obligaciones inmediatas por falta de recursos o activos líquidos.
- **Riesgo operacional**: errores de proceso, sistemas, personas o fallos internos que generan pérdidas.
- **Riesgo legal o regulatorio**: consecuencias adversas por cambios legislativos, sanciones o litigios.

Conociendo estos riesgos, una empresa puede diseñar un plan que actúe como contención, minimizando su impacto y mejorando su capacidad de reacción.



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 Nº 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,
Nº 94 - 23
Tel: +57 601 3000590 | +57 320 3657308

México DF, México

Av. Darwin Nº. 74, Interior 301,
Colonia Anzures, Ciudad de México
11590 México
Tel: +52 5541616885