EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

2025

SEPTIEMBRE

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.

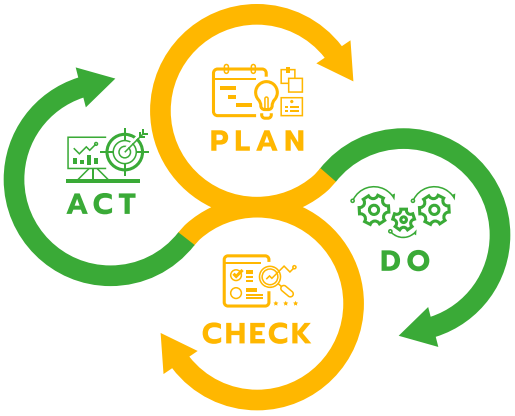
Plataforma ESG Innova

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

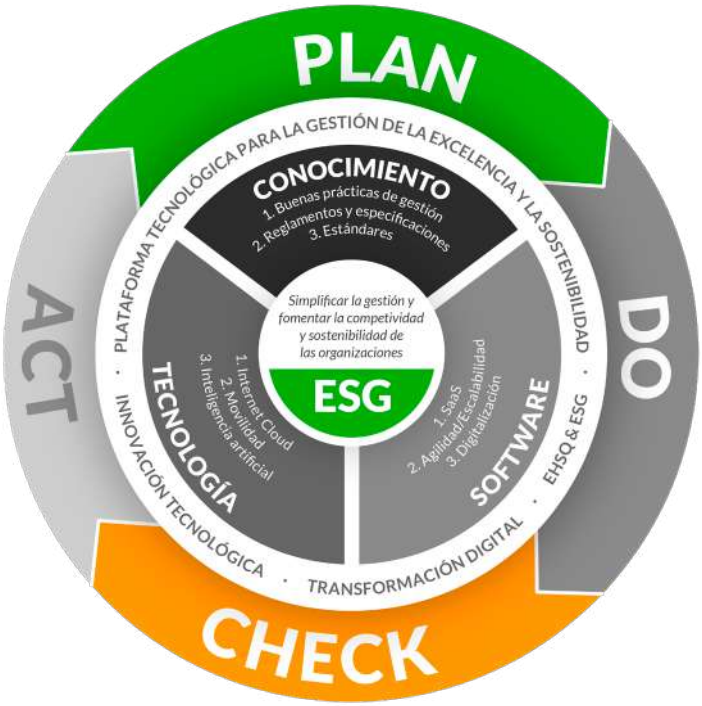
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ 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**

El coste de no implementar ISO 42001: riesgos reputacionales, regulatorios y de mercado

La inteligencia artificial ha revolucionado el panorama empresarial, pero su implementación sin apoyarse en un marco normativo adecuado puede resultar devastadora. El **coste de no implementar ISO 42001** va mucho más allá del riesgo de sanciones. Puede convertirse en una amenaza real que comprometa el cumplimiento regulatorio, la reputación y la viabilidad a largo plazo de la organización.

La transformación digital y el uso de nuevas tecnologías requieren un enfoque responsable que equilibre la innovación con la **gestión de riesgos**. El coste de no implementar ISO 42001 se materializa en múltiples dimensiones, que afectan a la competitividad, la reputación y la sostenibilidad financiera de las organizaciones.

ISO 42001: por qué es esencial para las organizaciones

- ISO 42001 representa el primer estándar internacional específicamente diseñado para **sistemas de gestión de inteligencia artificial**. Esta norma proporciona un marco estructurado para **identificar, prevenir, tratar y aprovechar los riesgos y oportunidades** asociados al desarrollo y uso de tecnologías de IA.

- La norma es **aplicable a cualquier organización que desarrolle, implemente o utilice sistemas de IA**, independientemente de su sector, tamaño o complejidad. Esto incluye desde startups tecnológicas hasta multinacionales, pasando por instituciones públicas y organizaciones de cualquier sector del tejido productivo.

Riesgos críticos: el coste de no implementar ISO 42001

- **ISO 42001 sigue la estructura de alto nivel y el modelo PDCA** (planificar, hacer, verificar, actuar), promoviendo la mejora continua para crear un marco ético, transparente y seguro para el uso de tecnologías de IA. Su implementación no solo mitiga riesgos, sino que facilita la integración con otros estándares como **ISO 27001** o ISO 9001, optimizando la gestión integral de la organización.

- **Ignorar esta norma implica asumir riesgos** que afectan a todos los niveles de la organización.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Cuáles son los beneficios de la ISO 9001 2026?

La versión proyectada para **ISO 9001:2026** apunta a reforzar lo que ya ofrece la versión vigente (2015) e incorporar nuevas exigencias para adaptarse al entorno empresarial actual. Con la globalización, la digitalización, el enfoque en riesgos y una mayor atención a stakeholders, las empresas que adopten este sistema de gestión de la calidad podrán obtener ventajas muy claras. En este artículo analizamos **11 beneficios de la ISO 9001** que harán que implantarla (o actualizarse a su versión 2026) sea una decisión estratégica.

1. Los beneficios de la ISO 9001 y el aumento de la satisfacción del cliente

ISO 9001 exige comprender y cumplir las **expectativas de los clientes**, además de medir su grado de satisfacción. Esto lleva a entregar productos y servicios que se ajusten mejor a lo que esperan, lo que se traduce en menos reclamaciones, mayor fidelidad y una reputación fortalecida.

2. Uno de los beneficios de la ISO 9001 clave: mejora de la calidad de productos y servicios

Con la norma, se estandarizan procesos y se establecen controles de calidad. La mejora continua es un pilar, por lo que los errores disminuyen, se mejora la **consistencia del producto/servicio** y se garantiza que lo entregado cumple con los requisitos esperados.

3. Reducción de costes sostenida en el tiempo

Aunque la implantación inicial tiene costes (tiempo, recursos, capacitación), el enfoque en procesos, la eliminación de redundancias, reprocesos y errores tiene como resultado una **mayor eficiencia y un uso óptimo de los recursos**, lo que permite reducir costes operativos a mediano y largo plazo.

4. Incremento del compromiso interno y satisfacción de los empleados

ISO 9001 considera a los empleados como **partes interesadas**. La claridad en responsabilidades, definición de roles, **comunicación efectiva** y participación en el sistema ayudan a que el personal esté más motivado, se sienta valorado y trabaje con mayor alineación hacia los objetivos de calidad de la empresa.

5. Cumplimiento de obligaciones de clientes y proveedores

En muchos sectores, especialmente los que operan en cadenas globales, clientes grandes solicitan que sus proveedores cuenten con certificaciones ISO 9001.

Cumplimiento ISO 27001: los 9 pasos esenciales para preparar tu certificación

Organizaciones de todo tipo, tamaño y sector manejan grandes cantidades de información. Se trata, en muchos casos, de datos sensibles, lo que obliga a implementar sistemas de gestión que garanticen elevados niveles de seguridad. En ese escenario, el **cumplimiento ISO 27001** se ha convertido en prioridad estratégica para conseguir una certificación que aporte garantías.

Implementar un **Sistema de Gestión de Seguridad de la Información** (SGSI) bajo ISO 27001 es un proceso estructurado que requiere planificación, compromiso y una hoja de ruta clara. Conseguir la certificación no solo **fortalece la posición competitiva de la organización**, sino que también demuestra a clientes y socios comerciales el compromiso con la protección de datos críticos.

¿Por qué el cumplimiento ISO 27001 es crucial para las organizaciones?

ISO 27001 es el estándar internacional más reconocido para establecer, implementar y mantener sistemas de gestión de seguridad de la información (SGSI). **Su propósito es proteger la confidencialidad, integridad y disponibilidad de la información** frente a amenazas internas y externas.

La norma **proporciona un marco sistemático para evaluar riesgos y aplicar controles necesarios para mitigarlos o eliminarlos**. La estructura de ISO 27001 se articula en 10 cláusulas principales que abarcan desde el contexto organizacional hasta la mejora continua, siguiendo la metodología del ciclo PDCA (Planificar-Hacer-Verificar-Actuar).

Cómo alcanzar el cumplimiento ISO 27001 paso a paso

La certificación que avala el cumplimiento ISO 27001 significa el **reconocimiento oficial de que un SGSI cumple con los requisitos internacionales más exigentes**, que la organización ha implementado controles efectivos de seguridad y mantiene un sistema de gestión maduro que protege la información de manera continuada.

Antes **es necesario superar una auditoría externa** realizada por un organismo certificador acreditado que compruebe el cumplimiento ISO 27001.

Gobierno de la IA: los 7 fundamentos clave de una gobernanza efectiva

La inteligencia artificial está transformando radicalmente la forma de operar de las organizaciones. Sin embargo, con ese poder surge la necesidad de establecer un **gobierno de la IA** que garantice un uso responsable y ético de esta tecnología. En ese escenario, la incorporación de la norma **ISO 42001** proporciona un marco específico para gestionar de forma ética, transparente y segura los sistemas de inteligencia artificial.

Más allá del cumplimiento regulatorio, el gobierno de la IA constituye **una herramienta para generar valor y diferenciarse en mercados altamente competitivos**. Al estructurar políticas claras, definir responsabilidades y asegurar una supervisión continua, las organizaciones pueden convertir la inteligencia artificial en un motor de innovación confiable y responsable.

¿Qué es el gobierno de la IA?

El gobierno de la IA es el conjunto de políticas, prácticas, normas y procesos que permiten a una organización **controlar el ciclo de vida completo de sus sistemas de inteligencia artificial**. Su finalidad es doble:

- **Minimizar riesgos** asociados a sesgos, falta de transparencia o incumplimiento normativo.
- **Maximizar beneficios**, garantizando que la IA actúe en coherencia con los valores de la organización y genere confianza en clientes, empleados y reguladores.

Lejos de ser un marco rígido, **el gobierno de la IA debe ser adaptable**. Cada organización debe diseñar su estructura en función de su sector, tamaño y contexto normativo. Pese a ello, los fundamentos son universales: ética, responsabilidad, calidad de datos, **gestión de riesgos**, cumplimiento, supervisión y soporte tecnológico.

Fundamentos clave del gobierno de la IA

La implementación exitosa de un marco de gobernanza de IA requiere la **integración de componentes interconectados**. Son los que proporcionarán una base estructural sólida para supervisar sistemas de inteligencia artificial de manera efectiva.

Calidad 5.0: cómo la inteligencia artificial y el factor humano transforman la excelencia operativa

La evolución tecnológica ha conducido a las organizaciones a un punto de inflexión sin precedentes. La **calidad 5.0** representa la convergencia entre inteligencia artificial avanzada, experiencia humana y transformación digital, redefiniendo los paradigmas de gestión que sustentan normas como **ISO 9001**. Esta realidad abre nuevas posibilidades para lograr la excelencia, la sostenibilidad y la mejora continua.

No se trata de una simple implementación tecnológica. Las organizaciones buscan **sistemas inteligentes que no sustituyan la capacidad humana, sino que la potencien** mediante el análisis predictivo, la monitorización continua y la toma de decisiones colaborativa. Este enfoque integral marca la diferencia entre digitalizar procesos existentes y transformar verdaderamente la gestión de la calidad.

Qué define a la calidad 5.0 y cómo ha evolucionado

La calidad 5.0 surge como evolución de la **calidad 4.0**. Si aquella se centraba en la automatización y la digitalización, la nueva etapa **integra IA, aprendizaje automático, IoT y análisis avanzado**, siempre bajo un enfoque centrado en las personas. Son cinco los pilares que en este contexto transforman la gestión tradicional:

- **Establece una colaboración entre humanos e IA**. La tecnología amplifica las capacidades analíticas, pero el juicio humano sigue siendo determinante.
- **Implementa análisis predictivo** y prescriptivo que anticipa fallos antes de manifestarse físicamente.
- **Se traduce en una hiperconectividad de sistemas**. Se crean flujos de datos en tiempo real que circulan entre procesos, clientes y proveedores.
- **Fomenta el aprendizaje continuo** mediante algoritmos que se adaptan automáticamente a nuevos patrones y contextos operacionales.
- **Prioriza el diseño centrado en el usuario**, garantizando interfaces intuitivas y procesos simplificados.

En resumen, mientras que enfoques previos se concentraban en la digitalización de procesos manuales, la calidad 5.0 crea ecosistemas inteligentes interconectados que aprenden y evolucionan continuamente. De esta forma, **la gestión reactiva cede paso a estrategias proactivas** que previenen problemas antes de su aparición.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Cómo decidir si la certificación del estándar ISO 42001 es la opción adecuada para su organización?

La inteligencia artificial se ha consolidado como una fuerza profundamente transformadora en el ámbito empresarial. Sin embargo, su rápido desarrollo plantea importantes desafíos relacionados con la ética, la transparencia y la gestión de riesgos. La **certificación del estándar ISO 42001** surge como respuesta eficaz para abordar estas preocupaciones y garantizar una implementación responsable de la IA.

La decisión de obtener la certificación del estándar ISO 42001 **requiere una evaluación cuidadosa de las necesidades de la organización**, del contexto regulatorio y de los objetivos estratégicos. Este análisis permitirá determinar si el marco normativo aportará valor real a la organización y justificará la inversión necesaria para su implementación.

Qué es el estándar ISO 42001

ISO 42001 es el **primer estándar de sistemas de gestión de la IA**. La norma ofrece a las organizaciones la orientación que necesitan para **utilizar la IA de forma responsable y eficaz**, incluso con una tecnología que evoluciona rápidamente. El estándar aborda aspectos críticos, entre ellos:

- **Gobernanza de la IA** y rendición de cuentas.
- Gestión de riesgos asociados a la IA.
- Transparencia y explicabilidad de los algoritmos.
- Calidad de los datos y protección de la privacidad.
- Cumplimiento de requisitos legales y regulatorios.
- Mejora continua e innovación responsable.

Sistemas de gestión de IA (SGIA) según ISO 42001

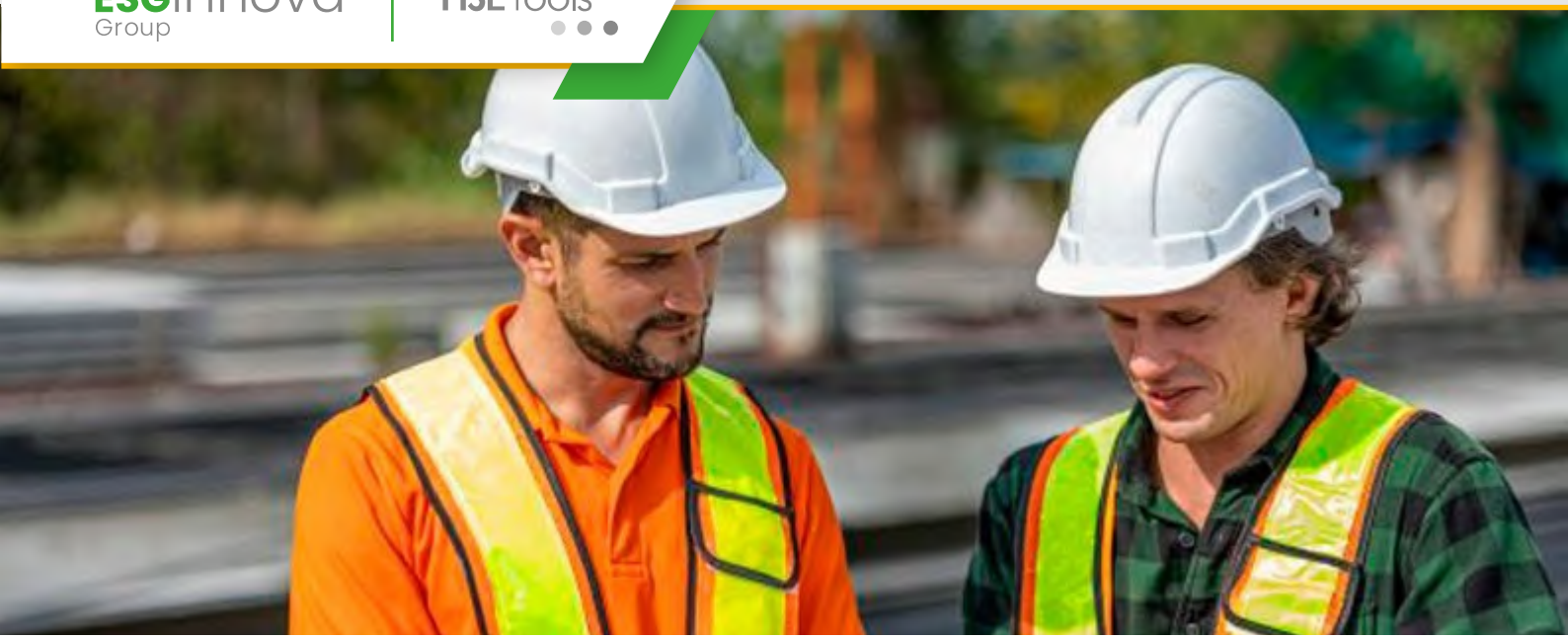
Según ISO 42001, un SGIA es un marco estructurado diseñado para ayudar a las organizaciones a gestionar el desarrollo, la implementación y el mantenimiento de sistemas de IA de manera responsable. Este sistema proporciona un enfoque sistemático que **integra la gestión de la IA con los objetivos estratégicos organizacionales**.

Un sistema de gestión de la IA efectivo **debe incorporar políticas claras, procedimientos documentados, asignación de responsabilidades** y mecanismos de monitoreo continuo.

ESGinnova
Group

HSE Tools

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



Cómo impulsar el cumplimiento y seguridad del contratista en 5 pasos

Una **gestión de contratistas** eficaz no solo impacta directamente en los indicadores de seguridad, sino que también determina el nivel de cumplimiento legal, fortalece la reputación corporativa y asegura la continuidad operativa. Pese a ello, el **cumplimiento y seguridad del contratista** representa uno de los mayores desafíos para aquellas empresas que apoyan parte de su actividad en fuerza laboral externa.

Lograr un nivel sólido de cumplimiento y seguridad del contratista es una labor compleja. Requiere adoptar **un enfoque estructurado, digitalizado y medible** que permita mejorar el desempeño de la seguridad en terceros. Por ello, no puede entenderse como un proceso aislado, sino como parte integral del sistema de **gestión HSE** de la organización.

Cumplimiento y seguridad del contratista: pasos para una gestión eficiente

Un fallo en la gestión del cumplimiento y seguridad del contratista puede derivar en accidentes graves, sanciones regulatorias y pérdida de confianza en la cadena de suministro. Para evitarlo, existen metodologías que, combinadas con una **plataforma de gestión HSE**, permiten **estructurar un ciclo de vida completo de la gestión del contratista**. Los siguientes son 5 pasos fundamentales en ese proceso

1. Planificación estratégica de los requisitos laborales

La base de cualquier programa efectivo de cumplimiento y seguridad del contratista radica en una planificación exhaustiva para **definir claramente los requisitos del proyecto antes de iniciar cualquier proceso de selección**. Esta fase debe incluir:

- **Evaluación de riesgos específicos**: identificar los peligros potenciales asociados a cada tarea. La **matriz de riesgos** debe incluir tanto riesgos inherentes al trabajo como aquellos derivados de la interacción entre diferentes contratistas.

- **Definición de competencias técnicas**: criterios específicos de certificación, experiencia y capacitación que deben cumplir los contratistas. Incluye acreditaciones sectoriales o permisos de trabajo específicos, por ejemplo, para trabajar en altura o en espacios confinados.

Aplicación HSE: ¿por qué merece la pena reemplazar Excel y documentos dispersos?

Una **aplicación HSE** se presenta como respuesta eficaz a los problemas de coordinación, control y eficiencia a los que se enfrentan muchas organizaciones que deben manejar grandes cantidades de información. En un entorno empresarial donde la **gestión de documentos** centralizada impulsa la productividad, acelera la toma de decisiones y fortalece el cumplimiento normativo, la digitalización de los procesos HSE representa una ventaja competitiva fundamental.

Las empresas dependen de hojas de cálculo, correo electrónico y documentos dispersos comprometen su eficiencia operativa y asumen riesgos innecesarios. Los costes derivados de incumplimientos normativos, multas por infracciones e incidentes evitables superan ampliamente la inversión inicial en tecnología. Una solución digital integrada elimina estos problemas y **proporciona control total sobre los procesos críticos de seguridad y salud laboral**.

Ventajas de una aplicación HSE frente a la gestión documental manual

El uso de una aplicación HSE **representa un salto cualitativo en la gestión de las organizaciones**. Sus beneficios van mucho más allá de la optimización de la **gestión documental**.

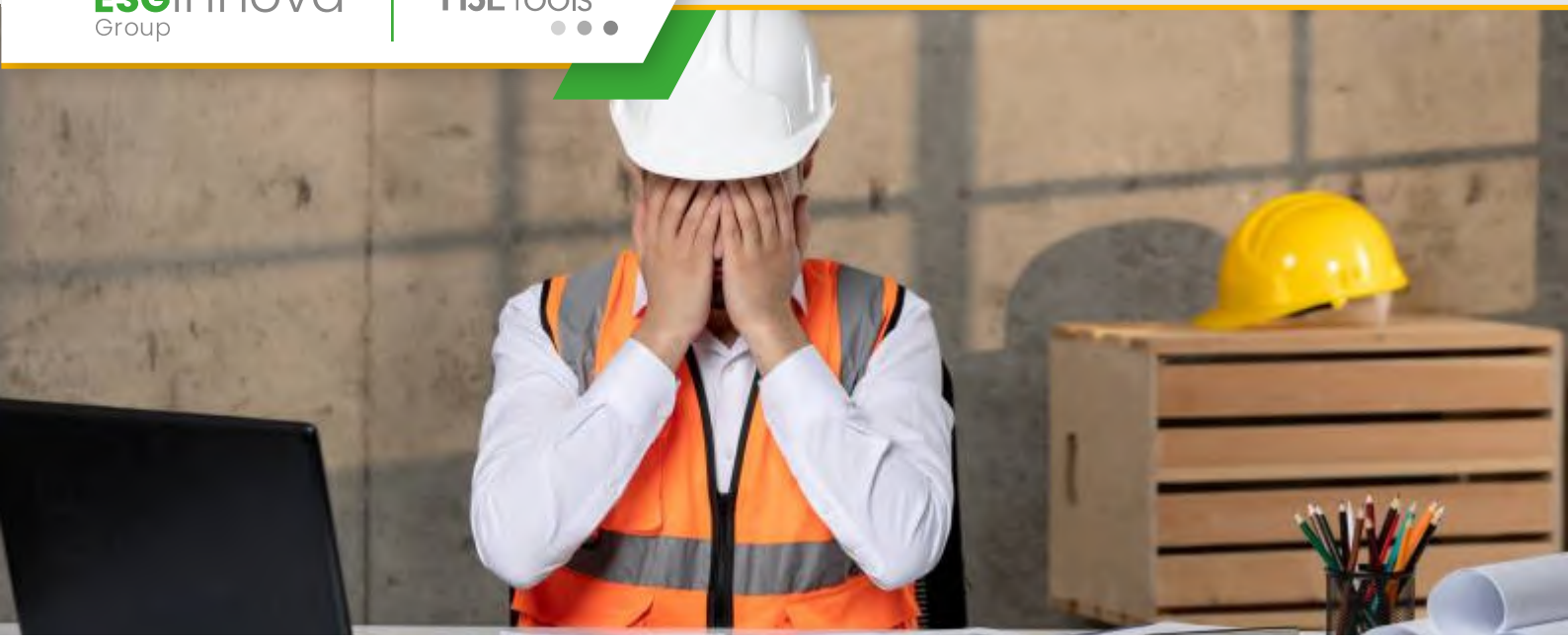
- **Reducción de los riesgos operativos y financieros**

Una aplicación HSE especializada **transforma la gestión reactiva en un enfoque preventivo**. El **software de salud, seguridad y medio ambiente** centraliza el seguimiento de incidentes, cuasi accidentes y acciones correctivas. Permite así identificar patrones de riesgo antes de que se materialicen en problemas graves, algo muy complicado cuando la información se maneja en hojas de cálculo. La automatización de recordatorios, la trazabilidad completa de acciones y el cumplimiento automatizado de plazos **eliminan riesgos financieros derivados de multas o sanciones** por incumplimiento normativo. Además, la reducción del número y gravedad de incidentes no solo protege a los trabajadores, sino que también evita costes asociados, como paradas de producción o daños reputacionales.

- **Automatización completa de procesos críticos**

Una aplicación HSE elimina las tareas manuales que consumen un tiempo valioso. Automatiza la programación de inspecciones, el registro de formaciones, la generación de informes y el seguimiento de acciones correctivas, entre otros aspectos. Esas horas que se liberan se pueden dedicar a actividades como la mejora de los procesos de seguridad y la implementación de medidas preventivas avanzadas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Sistemas de coacción para reducir la violencia en el lugar de trabajo

La **violencia en el lugar de trabajo** es un problema creciente que afecta a empresas de todos los sectores y tamaños. En 2022, se registraron 524 muertes relacionadas con este tipo de incidentes, lo que supuso un incremento del 9% respecto al año anterior. Estas cifras evidencian que no estamos ante casos aislados, sino frente a una tendencia preocupante que exige medidas preventivas urgentes.

Más allá de las estadísticas, la violencia laboral tiene consecuencias profundas: afecta a la integridad de los trabajadores, genera entornos hostiles, incrementa el **absentismo** y pone en riesgo la reputación corporativa. Ante este escenario, las empresas deben adoptar soluciones innovadoras que protejan a su personal y garanticen la continuidad de las operaciones. Una de las más efectivas son los **sistemas de coacción**, conocidos en inglés como *duress systems*.

¿Qué son los sistemas de coacción y cómo funcionan para reducir la violencia en el lugar de trabajo?

Los sistemas de coacción son **dispositivos de seguridad diseñados para enviar alertas silenciosas y discretas** cuando un trabajador se siente amenazado. Su principal ventaja es que permiten pedir ayuda sin que la persona agresora se percate, evitando que la situación escale.

Estos sistemas incluyen tres elementos clave:

- **Mecanismo de activación**: puede ser un botón oculto, un dispositivo portátil (como una pulsera o colgante) o una aplicación móvil.
- **Transmisión de la señal**: se realiza mediante radiofrecuencia o red celular, enviando el aviso a los equipos de seguridad internos o directamente a las autoridades.
- **Registro de datos**: los modelos más avanzados almacenan información sobre cada evento, lo que permite analizar patrones y fortalecer la prevención.

Hoy en día, gracias al **Internet de las Cosas (IoT)**, los sistemas de coacción ofrecen monitorización en tiempo real, integración con otras plataformas de seguridad y mayor capacidad de respuesta.

La violencia en el lugar de trabajo: una amenaza real

La **violencia en el lugar de trabajo** puede presentarse en múltiples formas: agresiones físicas, amenazas verbales, hostigamiento o comportamientos intimidatorios.

Gestión de contratistas y subcontratistas con software avanzado: simplifica procesos y evita riesgos

En un escenario empresarial globalizado, las organizaciones dependen cada vez más de fuerza laboral externa para mantener sus operaciones. Por ello, la **gestión de contratistas y subcontratistas** se ha convertido en un pilar fundamental para garantizar el cumplimiento normativo y la seguridad laboral. Esta realidad **obliga a las empresas a implementar sistemas que permitan supervisar con eficacia a todos los actores** involucrados en sus procesos productivos. Sin embargo, la gestión de contratistas y subcontratistas distribuidos en diferentes ubicaciones y proyectos presenta desafíos significativos.

Esa complejidad aumenta de forma exponencial cuando es necesario coordinar requisitos de cumplimiento diversos, mantener estándares de seguridad uniformes y generar informes para auditorías.

Las **soluciones digitales** especializadas emergen como herramientas que **transforman la gestión tradicional en procesos eficientes, automatizados y trazables**.

Principales desafíos en la gestión de contratistas y subcontratistas

La gestión de contratistas y subcontratistas implica enfrentarse a diferentes obstáculos que **pueden comprometer tanto la eficiencia operativa como el cumplimiento normativo**. Identificarlos es el primer paso para implementar soluciones que agreguen valor a la organización.

Complejidad operativa

Coordinar contratistas y subcontratistas en múltiples proyectos simultáneos representa uno de los mayores retos organizacionales. Cada entidad opera bajo sus propios estándares, cronogramas y metodologías, creando un ecosistema complejo donde mantener la coherencia se vuelve extremadamente difícil.

Dispersión geográfica

Gestionar contratistas en **ubicaciones remotas** o dispersas **requiere sistemas que permitan supervisión remota efectiva** sin comprometer la calidad de ese control. La falta de presencia física no puede traducirse en una reducción de los estándares de cumplimiento.

Informes de cumplimiento HSE: cómo evitar errores costosos y simplificar la documentación

Una gestión documental eficiente es clave en los **programas HSE** de las organizaciones. En esa gestión, los **informes de cumplimiento** constituyen la evidencia tangible de que se mantienen unos estándares adecuados de seguridad, salud ocupacional y protección ambiental. Su correcta elaboración no solo garantiza el cumplimiento normativo, sino que protege a la empresa frente a posibles sanciones regulatorias y refuerza la confianza de empleados, clientes y partes interesadas.

La realidad de muchas organizaciones, sin embargo, refleja una gestión fragmentada, con documentación dispersa entre múltiples plataformas, herramientas obsoletas y **procesos manuales** propensos al error. **La desorganización compromete la eficiencia operativa y expone a las empresas a riesgos económicos y reputacionales**.

Frente a ella, la digitalización se consolida como la solución más efectiva para superar estos desafíos.

Riesgos y consecuencias de informes de cumplimiento deficientes

Errores, inexactitudes o ausencia de documentos y registros pueden tener **consecuencias severas para la organización**:

❖ Impacto económico directo

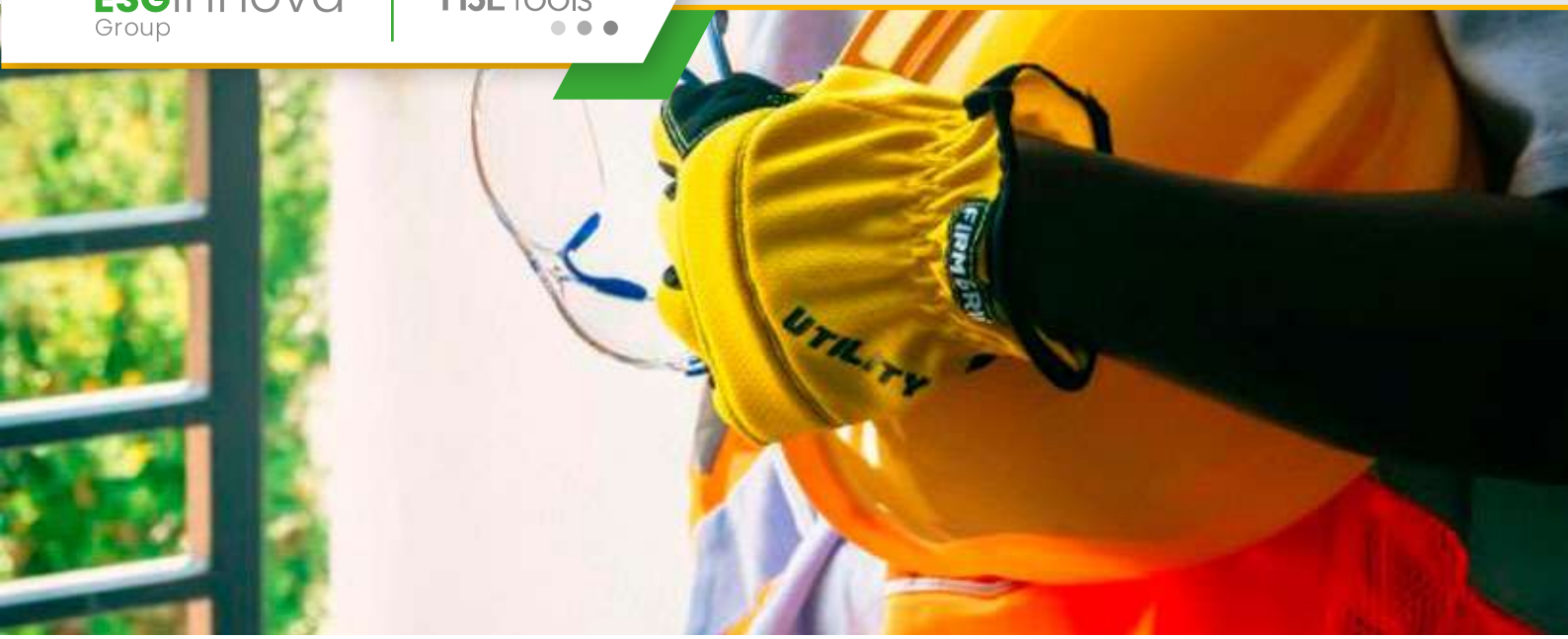
Una **mala gestión documental** puede suponer no solo multas y sanciones regulatorias, también la pérdida de contratos. Instituciones públicas y organizaciones privadas exigen cada vez más evidencias documentales sólidas, donde los informes de cumplimiento representan un requisito indispensable. **Una empresa que no puede demostrar sus estándares HSE mediante documentación rigurosa pierde ventaja competitiva**.

❖ Riesgos operacionales y reputacionales

Informes de cumplimiento sesgados o ineficientes generan retrasos en investigaciones de incidentes y **limitan la capacidad de implementar acciones correctivas efectivas**. Esa circunstancia puede tener graves repercusiones:

- Repetición de incidentes similares.
- Pérdida de confianza del personal.
- Deterioro del clima laboral.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Programa de EPI: claves para la inspección, ajuste y sustitución de equipos de protección

En sectores donde existe una exposición a riesgos físicos, químicos o ambientales, contar con un **programa de EPI** sólido marca la diferencia entre una **gestión de riesgos** efectiva y la reacción tardía. Sin embargo, diseñar y mantener un plan de gestión de equipos de protección individual requiere actualización constante, capacidad de adaptación a las condiciones ambientales cambiantes y un enfoque preventivo alineado con la normativa.

En España y en la Unión Europea, el marco legal que regula el uso y la gestión de los **equipos de protección en el lugar de trabajo** lo conforman el Reglamento 2016/425 de la UE, el Real Decreto 773/1997 sobre utilización de equipos de protección individual y, en el ámbito de la construcción, el Real Decreto 1627/1997. Estas disposiciones **obligan a los empleadores a seleccionar, proporcionar, formar y garantizar el correcto uso de los EPI**.

No cumplir con ellas no solo implica sanciones, sino que compromete la seguridad y la productividad de toda la organización.

Elementos clave del programa de EPI

Un programa de EPI sólido es proactivo, es decir, **anticipa riesgos, planifica recursos y establece protocolos para reducir la probabilidad de fallos**. Se trata de adaptarse a las condiciones cambiantes y prevenir problemas antes de que interrumpan las operaciones o comprometan la seguridad de los trabajadores. La implementación efectiva requiere considerar aspectos como la exposición al frío, la reducción de luz natural, los riesgos de condensación y el uso de múltiples capas de ropa que pueden interferir con el rendimiento del equipo de protección. **Un programa de EPI integral debe incluir**:

- **Identificación de riesgos de seguridad y salud** específicos por puesto y tarea.
- Selección de EPI certificados conforme a la normativa.
- Formación y entrenamiento en uso, ajuste y mantenimiento.
- Sistemas de inspección y reposición basados en criterios objetivos.
- Registro y trazabilidad de pruebas, mantenimientos y caducidades.

La clave está en que el programa de EPI evolucione con las circunstancias: desde un cambio en los procesos productivos hasta variaciones del clima que pueden alterar la eficacia de accesorios como guantes, gafas o arneses.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Plataforma para gestión de contratistas: 7 funciones imprescindibles que debe incluir

En un entorno empresarial marcado por la complejidad, contar con una **plataforma para gestión de contratistas** no es una opción, sino una necesidad. La variedad de proveedores, la dispersión geográfica de los proyectos y un marco regulatorio cada vez más estricto generan un escenario en el que la improvisación puede derivar en incumplimientos, sanciones o pérdidas de eficiencia.

Las organizaciones necesitan herramientas digitales que les permitan centralizar la información, automatizar procesos y garantizar la seguridad de las operaciones. **Una plataforma avanzada no solo reduce riesgos, también facilita la transparencia**, mejora la relación con los contratistas y aporta visibilidad a la alta dirección para tomar decisiones basadas en datos.

7 funciones imprescindibles en una plataforma para gestión de contratistas

Para que una plataforma para gestión de contratistas sea efectiva, debe integrar funcionalidades que aborden los principales desafíos operacionales a los que deben enfrentarse las organizaciones modernas. Las características que se detallan a continuación **optimizan procesos individuales y crean un ecosistema cohesionado** que transforma la gestión de contratistas en una ventaja competitiva.

1. Incorporación automatizada de contratistas

La **incorporación de contratistas** representa el primer punto crítico en la relación con la fuerza laboral externa. Una plataforma para gestión de contratistas eficiente debe **automatizar este proceso, eliminando las tareas manuales repetitivas** y reduciendo los tiempos de activación. Para ello, debe incorporar funcionalidades como las siguientes:

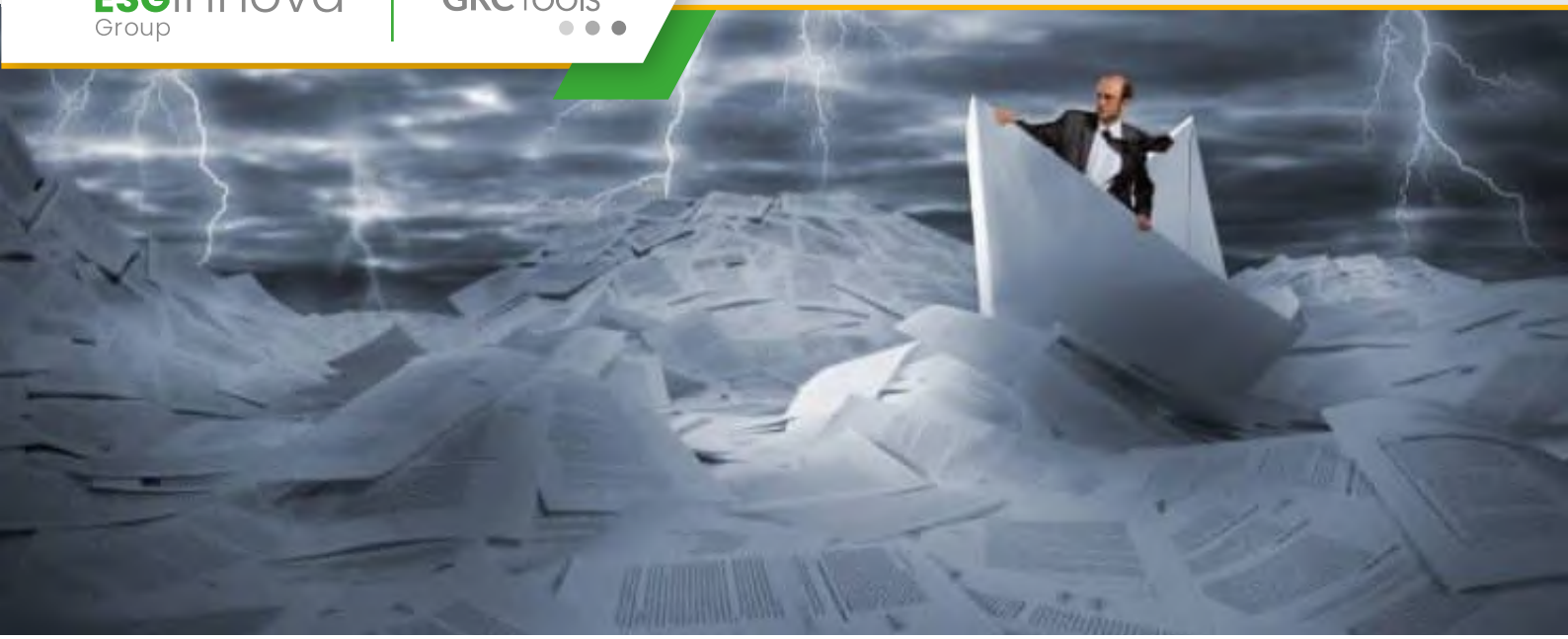
- Recopilación automatizada de documentación legal y técnica.
- Verificación digital de credenciales y certificaciones.
- Validación automática de seguros y garantías.
- **Flujos de trabajo** configurables según tipo de contratista.
- Integración con bases de datos gubernamentales y sectoriales.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

ESGinnova Group

GRCTools

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



¿Cómo gestionar los riesgos empresariales visibles y ocultos?

En la actualidad, las organizaciones se enfrentan a un panorama cada vez más complejo de **riesgos empresariales**. Algunos son claramente visibles —como sanciones regulatorias, fraudes financieros o incidentes de ciberseguridad—, mientras que otros permanecen ocultos bajo la superficie, como problemas en la cadena de suministro, impactos reputacionales, fallos culturales internos o dependencias tecnológicas críticas. Tal como ocurre con un iceberg, la parte más peligrosa suele ser la que no se ve a simple vista.

Ignorar estos riesgos invisibles puede tener **consecuencias devastadoras**: interrupciones operativas, pérdida de clientes, sanciones regulatorias o incluso la inviabilidad del negocio. Por ello, las empresas deben evolucionar desde modelos tradicionales de gestión hacia marcos integrados que permitan identificar, anticipar y abordar tanto los riesgos evidentes como los que se ocultan en el entorno interno y externo.

El nuevo panorama de los riesgos empresariales

El ecosistema global está dominado por amenazas ambientales, sociales y tecnológicas que amplían la lista de **riesgos empresariales** a considerar. Entre los más relevantes destacan:

- **Ciberinseguridad y desinformación**, con un impacto creciente en la confianza y en la continuidad de operaciones.
- **Riesgos climáticos**, como fenómenos meteorológicos extremos que alteran cadenas de suministro y entornos productivos.
- **Pérdida de biodiversidad y escasez de recursos naturales**, con repercusiones regulatorias y reputacionales.
- **Riesgos regulatorios emergentes**, derivados de normativas como la CSRD, la CSDDD o la AI Act en la Unión Europea.

Estos riesgos, aunque diversos en origen, comparten un mismo denominador común: están interconectados y pueden multiplicar su impacto si no se abordan desde una visión integral.

Riesgos visibles vs. riesgos ocultos

Los riesgos visibles suelen ser los más atendidos: **auditorías, incidentes financieros, brechas de datos o incumplimientos normativos**. Son riesgos cuantificables, con métricas claras y consecuencias inmediatas. En cambio, los riesgos ocultos son más difíciles de detectar.

Cuestiones clave para la Alta Dirección en gobernanza corporativa

La **gobernanza corporativa** ha evolucionado de manera significativa en las últimas décadas. Lo que antes era un marco centrado principalmente en la transparencia financiera, hoy se ha transformado en un sistema mucho más complejo que exige a los **consejos de administración** un rol activo en la supervisión de múltiples áreas: estrategia, riesgos, sostenibilidad, ciberseguridad, compensación ejecutiva y relación con los grupos de interés.

Impulsada por crisis financieras, escándalos empresariales y nuevas regulaciones, la **gobernanza corporativa** se ha convertido en un pilar fundamental para garantizar la sostenibilidad y la confianza en los mercados. En 2025, los consejos enfrentan un escenario desafiante, marcado por la volatilidad económica, la presión de los reguladores, el activismo accionarial y la creciente relevancia de los criterios ESG (medioambientales, sociales y de gobernanza).

Funciones esenciales del consejo de administración

En medio de esta complejidad, las juntas directivas deben mantener el foco en cinco funciones esenciales que constituyen la base de una gobernanza sólida:

01. Selección y compensación de la alta dirección.

02. Supervisión de la estrategia de negocio.

03. Gestión y supervisión de riesgos.

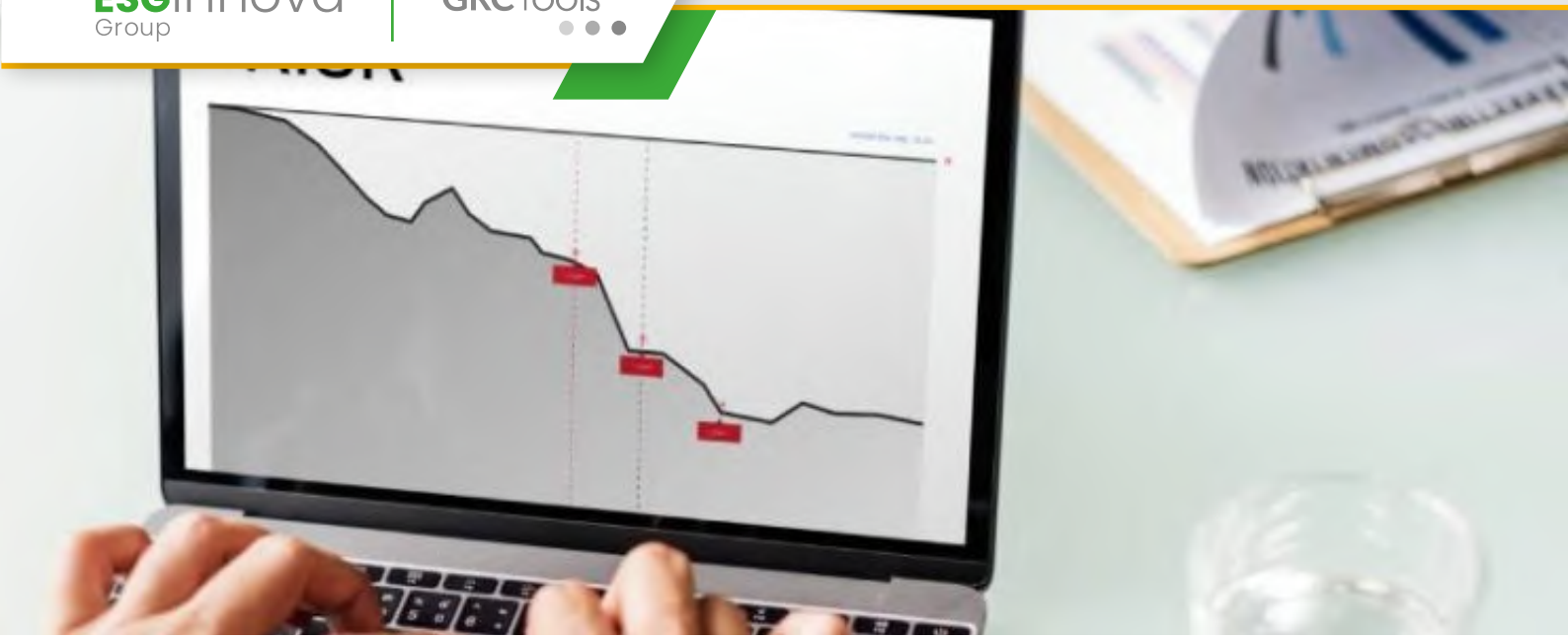
04. Construcción de credibilidad con inversores y stakeholders.

05. Autoevaluación de la composición y procesos del consejo.

Estas funciones permiten alinear los intereses de la empresa con los de los accionistas y otros grupos de interés, garantizando que la organización opere con integridad, eficiencia y visión de largo plazo.

Selección y compensación de la dirección

El proceso de **sucesión del CEO** se ha convertido en un tema crítico para los consejos. La alta rotación en puestos directivos y la presión de los activistas exigen a las empresas planes de sucesión robustos que aseguren continuidad y estabilidad. Casos como el de **Disney** ilustran la importancia de contar con una estrategia clara en esta materia.



10 metodologías de análisis de riesgos más importantes

El **análisis de riesgos** se ha convertido en un pilar estratégico para cualquier organización que busque garantizar su sostenibilidad y competitividad en un mundo cada vez más incierto. Crisis financieras, incidentes de ciberseguridad, disrupciones en cadenas de suministro y desastres naturales han demostrado que los riesgos son inevitables, pero su **impacto puede minimizarse si se gestionan de forma adecuada**.

La importancia de aplicar metodologías de análisis de riesgos

Contar con un enfoque estructurado de gestión de riesgos permite a las empresas **anticiparse a amenazas, priorizar recursos y tomar decisiones informadas**. Para lograrlo, existen distintas **metodologías de análisis de riesgos**, cada una con enfoques, técnicas y aplicaciones específicas.

En este artículo presentamos las **10 metodologías de análisis de riesgos más importantes**, junto con ejemplos de uso en diferentes sectores, para ayudarte a seleccionar la que mejor se adapta a tu organización.

1. Análisis de Riesgos y Puntos Críticos de Control (HACCP)

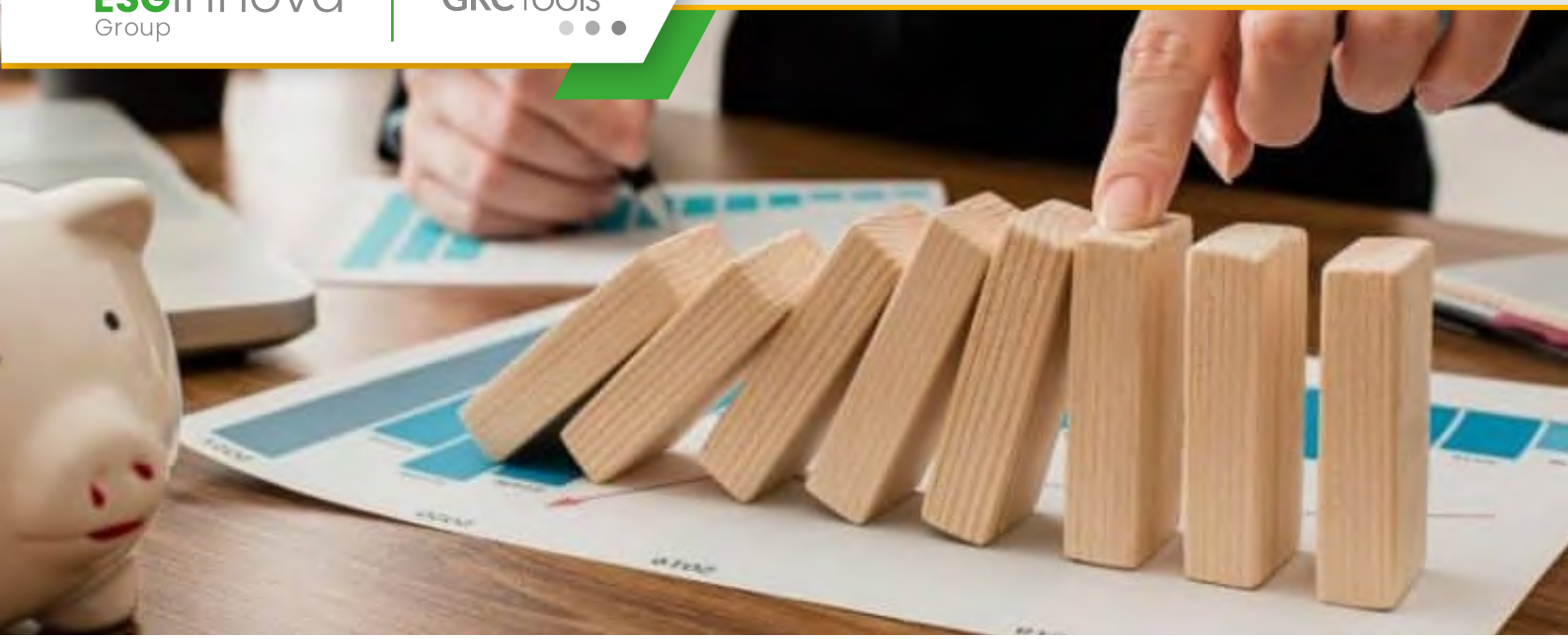
Una de las principales metodologías de análisis de riesgos es el **HACCP**. Este es indispensable en la industria alimentaria y manufacturera. Se centra en **identificar peligros** —físicos, químicos o biológicos— en las etapas de producción y establecer **controles preventivos** en los puntos críticos.

Ejemplo: una empresa de envasado de alimentos puede usar HACCP para verificar la correcta temperatura de almacenamiento y evitar contaminaciones que comprometan la seguridad del consumidor. Su implementación reduce riesgos sanitarios y asegura el cumplimiento de normativas internacionales.

2. Análisis Modal de Fallos y Efectos (AMFE o FMEA)

El **AMFE** evalúa qué podría fallar en un producto o proceso, cuáles serían sus consecuencias y cómo prevenirlo. Permite asignar un **número de prioridad de riesgo** para ordenar las acciones correctivas.

Ejemplo: en la industria automotriz se aplica para detectar fallos en piezas antes de que salgan al mercado, evitando costosos recalls. El beneficio principal es la **confiabilidad y seguridad** de los productos.



3 claves para proteger tu empresa con una gestión de riesgos efectiva

El entorno empresarial actual está lleno de cambios rápidos, desafíos inesperados y una competencia cada vez más intensa, lo que obliga a las organizaciones a contar con una estrategia sólida que les permita anticiparse y reaccionar con eficacia. La **gestión de riesgos efectiva** se ha convertido en un factor determinante para sobrevivir, haciendo a las empresas crecer con solidez y aprovechar oportunidades en entornos cambiantes.

Una gestión de riesgos adecuada no se limita a reaccionar cuando ocurre un problema, sino que permite preverlo, analizarlo y reducir su impacto antes de que comprometa la estabilidad de la empresa. De hecho, las compañías que aplican este enfoque logran fortalecer su **resiliencia organizacional**, mejorar su competitividad y transmitir confianza a clientes, inversores y empleados.

En este artículo vamos a profundizar en **tres claves esenciales** que te ayudarán a implementar una gestión de riesgos robusta, práctica y alineada con los objetivos estratégicos de tu empresa.

1. Identificar y priorizar los riesgos

El primer paso de cualquier **gestión de riesgos efectiva** es conocer con claridad cuáles son las amenazas que pueden afectar a la organización. Esta fase de identificación es fundamental, ya que permite visualizar tanto los riesgos internos como los externos, y diseñar un mapa que sirva como punto de partida para su evaluación.

Algunos de los riesgos más comunes a los que se enfrentan las empresas son:

- **Riesgos financieros**: fluctuaciones económicas, problemas de liquidez o impagos de clientes clave.
- **Riesgos operativos**: interrupciones en la cadena de suministro, errores humanos, fallos en la producción.
- **Riesgos tecnológicos**: ciberataques, brechas de seguridad o fallos en sistemas críticos.
- **Riesgos legales y normativos**: sanciones por incumplimiento de leyes o cambios regulatorios inesperados.
- **Riesgos estratégicos**: aparición de nuevos competidores, cambios en los hábitos de consumo o irrupción de tecnologías disruptivas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué es el GenAI en cumplimiento normativo?

El **cumplimiento normativo** siempre ha sido una de las áreas más desafiantes para las organizaciones. Lejos de ser una tarea inspiradora, las **auditorías de cumplimiento** suelen asociarse con procesos lentos, costosos y tediosos. El volumen de datos que debe revisarse, las presiones por cumplir con los plazos y el riesgo constante de errores humanos convierten esta labor en una carga pesada para los equipos de cumplimiento. Sin embargo, la llegada del **Generative Artificial Intelligence (GenAI)** está cambiando este escenario.

En este artículo analizaremos **qué es el GenAI en cumplimiento normativo**, cuáles son sus principales beneficios, cómo puede implementarse de manera efectiva y qué retos plantea para las empresas. El objetivo no es caer en la moda pasajera, sino entender cómo esta tecnología puede convertirse en un verdadero **aliado estratégico** para la gestión de riesgos y la transparencia corporativa.

Los problemas tradicionales de las auditorías de cumplimiento

Antes de valorar cómo la **inteligencia artificial generativa** puede revolucionar el sector, es importante repasar los principales obstáculos de las auditorías tradicionales:

- **Exceso de datos**: un proceso de auditoría implica revisar documentos, políticas, correos electrónicos, registros de transacciones y un sinfín de información. Analizar todo manualmente es prácticamente imposible.

- **Plazos y recursos limitados**: los equipos de cumplimiento suelen trabajar con plantillas reducidas y presupuestos ajustados, lo que incrementa la presión para entregar informes en tiempo y forma.

- **Errores humanos**: cuanto más manual es un proceso, mayor es la posibilidad de pasar por alto información clave. Esto puede derivar en **multas regulatorias** o sanciones que afecten la reputación de la empresa.

El resultado de este cóctel suele ser el mismo: las auditorías se convierten en un simple **ejercicio de verificación de casillas**, perdiendo el foco en la **gestión preventiva de riesgos**.

GenAI en cumplimiento normativo: un cambio de paradigma

La irrupción del **GenAI en cumplimiento normativo** representa un salto cualitativo. A diferencia de las herramientas tradicionales de automatización, el GenAI es capaz de **analizar grandes volúmenes de datos estructurados y no estructurados.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué es la Ley Sox?

La **Ley Sarbanes-Oxley (Ley SOX)**, aprobada en 2002 en Estados Unidos tras los escándalos financieros de Enron, WorldCom y Tyco, transformó radicalmente la manera en que las empresas que cotizan en bolsa gestionan su información financiera. Su objetivo principal es **proteger a los inversionistas** garantizando la **transparencia y fiabilidad de los estados financieros**, así como fortalecer la responsabilidad de los directivos frente a posibles fraudes o manipulaciones contables.

Más de dos décadas después de su aprobación, la **Ley SOX** sigue siendo un referente mundial en materia de **gobierno corporativo, control interno y auditoría financiera**, y continúa marcando el estándar de cómo deben gestionarse los riesgos relacionados con la información financiera en grandes corporaciones.

Principales objetivos de la Ley SOX

La **Ley SOX** busca devolver la confianza en los mercados financieros a través de cuatro pilares fundamentales:

- **Transparencia**: asegurar que los informes financieros reflejen la realidad de la situación económica de la empresa.
- **Responsabilidad**: los directivos y el CEO/CFO deben certificar personalmente la veracidad de los estados financieros.
- **Control interno**: las organizaciones deben implementar y mantener sistemas de control robustos para detectar y prevenir errores o fraudes.
- **Supervisión externa**: se refuerza el papel de los auditores independientes y del regulador, el **Public Company Accounting Oversight Board (PCAOB)**.

El alcance de la Ley SOX: la sección 404

Uno de los aspectos más exigentes de la **Ley SOX** es la **Sección 404**, que obliga a las empresas a documentar, evaluar y certificar la efectividad de sus **controles internos sobre la información financiera** (ICFR, por sus siglas en inglés).

El problema es que, en la práctica, muchas compañías incluyen **demasiados controles en el alcance**, lo que genera programas sobredimensionados, costosos y poco eficientes.

Se habla entonces de un **"alcance inflado"** que no siempre aporta valor, pero sí incrementa la carga de trabajo para los equipos de auditoría interna y compliance.

Implicaciones de la IA en la Auditoría de control interno

La transformación digital ha revolucionado la forma en que las organizaciones gestionan sus procesos, riesgos y controles. En este contexto, la **auditoría de control interno** se enfrenta a un cambio trascendental impulsado por la irrupción de la **inteligencia artificial (IA)**. No se trata únicamente de incorporar nuevas herramientas tecnológicas, sino de redefinir el papel del auditor interno y el alcance mismo de los mecanismos de aseguramiento.

En los últimos años, el debate sobre el impacto de la IA en auditoría ha crecido de manera notable. Desde foros profesionales hasta informes de organismos internacionales, todos coinciden en que la IA ofrece **oportunidades sin precedentes**: más cobertura, velocidad en la detección de anomalías y una visión predictiva de los riesgos. Sin embargo, también plantea **nuevos retos** que no pueden ignorarse: sesgos en los modelos, falta de transparencia en los algoritmos y dependencia tecnológica. Este artículo analiza de manera práctica las principales implicaciones de la IA en la auditoría de control interno y cómo esta combinación puede aportar valor real a las organizaciones.

Nuevas capacidades en auditoría

La IA amplía las capacidades de la auditoría al permitir:

- **Cobertura plena en lugar de muestreo**: ya no es necesario revisar solo una muestra de transacciones; la IA puede analizar el **100 % de las operaciones** para identificar irregularidades.

- **Detección de anomalías en tiempo real**: los algoritmos monitorean flujos operativos y disparan alertas cuando detectan patrones atípicos que podrían indicar fraude, errores o brechas de control.

- **Capacidad predictiva**: al analizar datos históricos y actuales, la IA ayuda a anticipar posibles fallos en los controles internos antes de que ocurran.

- **Automatización de tareas repetitivas**: actividades como la extracción de datos, conciliaciones o rastreo documental pueden ejecutarse de forma automática, liberando tiempo para que el auditor se enfoque en análisis de mayor valor.

Estas capacidades permiten que la **auditoría de control interno** evolucione hacia un modelo más continuo y proactivo, dejando atrás el enfoque retrospectivo que tradicionalmente se centraba en detectar errores una vez ocurridos.

Caso práctico: IA en la detección de fraude

Imaginemos una entidad financiera que procesa millones de transacciones diarias.

¿Cuál es el rol de la IA en la gestión de riesgos financieros?

En el dinámico mundo de las finanzas, la **gestión de riesgos financieros** es un aspecto clave para garantizar la estabilidad y la confianza de los mercados. Factores como la volatilidad económica, los ciberataques, el fraude y los cambios regulatorios hacen que las instituciones financieras deban adaptarse con rapidez a escenarios cada vez más complejos.

En este contexto, el **rol de la IA en la gestión de riesgos financieros** se ha consolidado como un elemento transformador. La inteligencia artificial permite a bancos, aseguradoras y firmas de inversión no solo anticiparse a amenazas, sino también reaccionar en tiempo real para mitigar su impacto. Su doble función —predictiva y reactiva— convierte a la IA en un aliado estratégico para la estabilidad financiera global.

El rol de la IA en la gestión de riesgos financieros: la IA como motor de prevención

El primer gran aporte de la IA es su capacidad para **anticipar riesgos antes de que ocurran**. Gracias al aprendizaje automático y la analítica predictiva, los modelos de IA procesan enormes volúmenes de datos estructurados y no estructurados, detectando patrones que pueden pasar inadvertidos para el ojo humano.

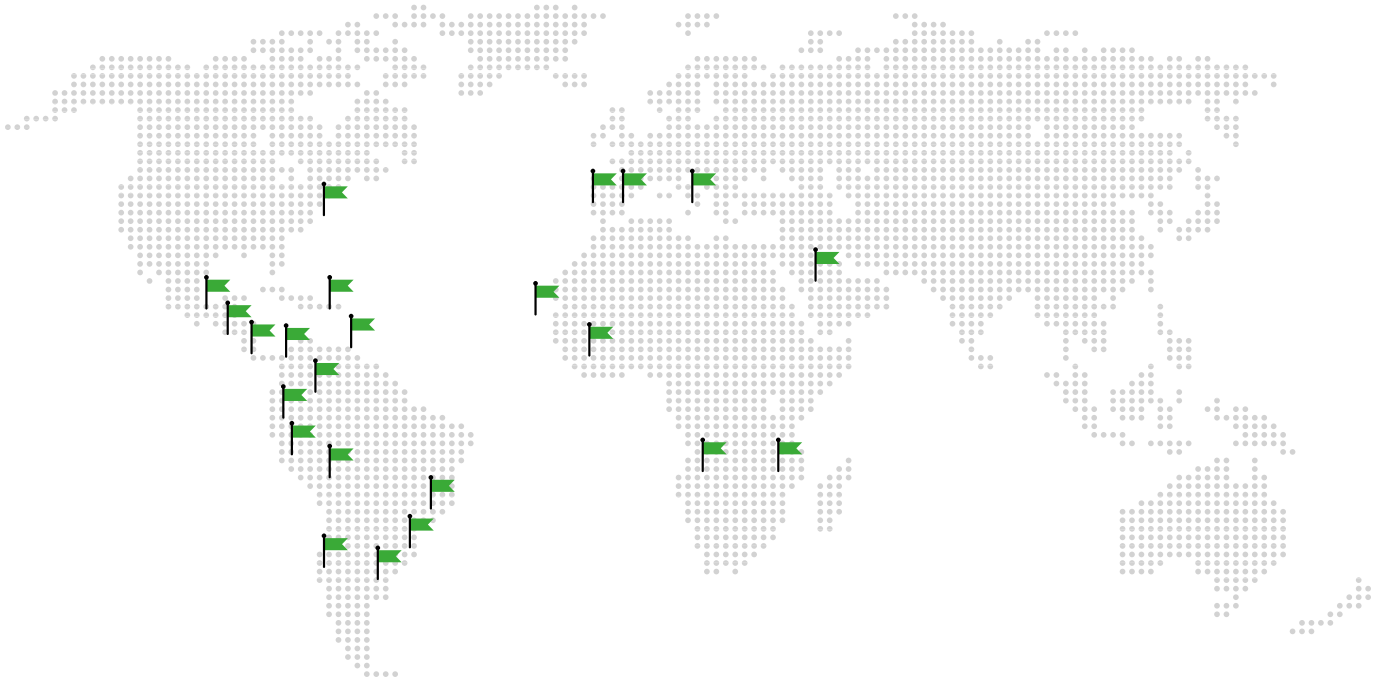
- **Evaluación de crédito:** los algoritmos de IA van más allá de los modelos tradicionales de scoring. Analizan hábitos de consumo, comportamiento en tiempo real y fuentes externas de información para construir perfiles de riesgo más precisos y dinámicos.

- **Riesgos de liquidez y reputación:** mediante la correlación de indicadores financieros y externos (como noticias o redes sociales), la IA permite anticipar posibles crisis de liquidez o amenazas a la reputación corporativa.

En un sector donde cada segundo cuenta, esta capacidad de predicción aporta ventajas competitivas decisivas.

Detección y prevención del fraude

El fraude financiero es una de las principales amenazas para las entidades del sector. Las soluciones tradicionales, basadas en reglas estáticas, no logran seguir el ritmo de los delincuentes, que emplean métodos cada vez más sofisticados.



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