EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

2025

AGOSTO

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.

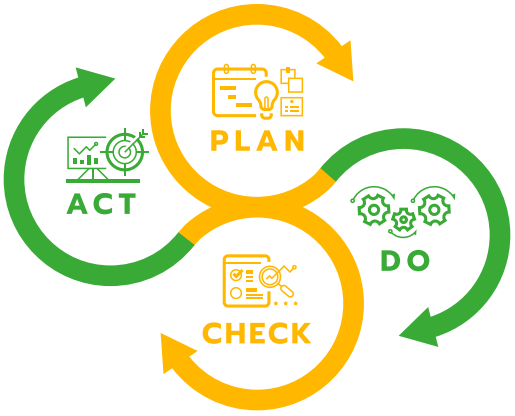
Plataforma ESG Innova

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

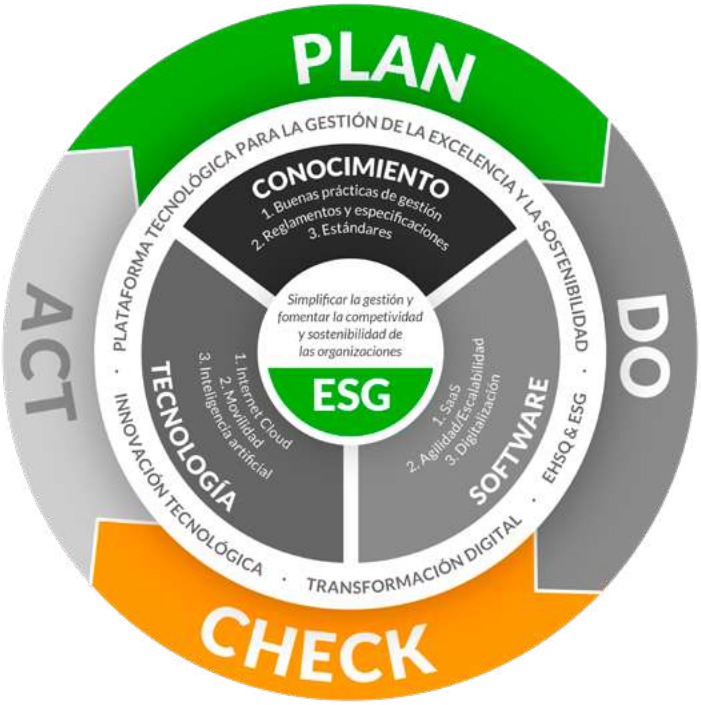
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ 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

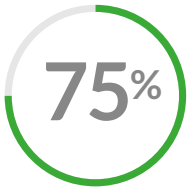
Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento.

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

Menos de tiempo de resolución de una acción correctiva

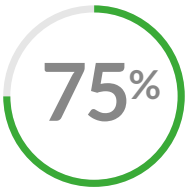
Menos de tiempo de preparación de las reuniones de gestión



Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

Menos de intercambios de documentación física entre sedes y dptos.



Menos de costes indirectos derivados de la gestión documental

La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento

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

Más capacidad de resolución de problemas del sistema de gestión

Más de trabajadores implicados en la gestión del sistema

ESGinnova Group

ISOTools

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

7 beneficios del software de control de calidad para cumplir con ISO y mejorar la gestión

La digitalización de los sistemas de gestión de calidad supone una evolución natural en el cumplimiento de requisitos normativos de las organizaciones. Contar con un **software de control de calidad** contribuye a optimizar procesos, reducir errores y alinear el sistema de gestión con los requisitos de normas como **ISO 9001**.

Implementar un **sistema de gestión de calidad** (SGC) de forma manual puede requerir grandes inversiones de tiempo y recursos. El uso de herramientas digitales especializadas permite **automatizar tareas, mejorar el acceso a la información y facilitar la toma de decisiones** basadas en datos reales. Son solo algunos de los beneficios que aporta la tecnología en el control de la calidad.

Ventajas de un software de control de calidad

El software de control de calidad es una plataforma tecnológica diseñada para gestionar documentos, evaluar el desempeño, automatizar procesos y asegurar el cumplimiento de **normas ISO**. Incorpora diferentes funcionalidades que contribuyen a **crear un entorno de mejora continua** donde la calidad se convierte en una práctica diaria.

1. Documentación centralizada, segura y accesible

La **gestión documental** (recogida en la cláusula 7.5 de ISO 9001) es una piedra angular del sistema de calidad. Con un software especializado, todos los documentos clave, desde procedimientos a instrucciones o registros, se almacenan en **un repositorio único, seguro y fácilmente accesible**.

La centralización **evita duplicidades, pérdida de versiones o errores de control**. Además de ello, facilita la trazabilidad de la documentación y permite configurar permisos por roles para proteger la información sensible. En términos de cumplimiento ISO, tener la documentación organizada y disponible facilita la preparación para auditorías.

2. Automatización de flujos de trabajo

Las tareas manuales son lentas, propensas a errores y consumen tiempo. Un software de control de calidad **resuelve estos problemas, automatizando tareas** como:

- Aprobación y revisión de documentos.
- Planificación de auditorías internas.

Ley de IA de la UE: cómo la ISO 42001 ayuda a las empresas a cumplir sus requisitos

La **Ley de IA de la UE** constituye un hito normativo sin precedentes en la regulación de sistemas de inteligencia artificial. Establece un marco exhaustivo que clasifica los sistemas de IA según su nivel de riesgo y define obligaciones específicas para cada categoría. Las organizaciones, que deben enfrentan el desafío de alinear sus operaciones con estos nuevos requerimientos legales, encuentran en la norma **ISO 42001** un aliado de gran valor.

ISO 42001 es el **primer estándar de sistemas de gestión de IA** del mundo. **Proporciona un marco estructurado para implementar sistemas de gestión de inteligencia artificial** que no solo cumplen con la regulación europea, sino que también establecen las bases para una gobernanza responsable y sostenible de la IA.

Claves de la Ley de IA de la UE

La Ley de IA de la UE, aprobada en 2024, es el primer marco regulatorio integral para la inteligencia artificial a nivel mundial. Esta normativa adopta un enfoque basado en riesgos que **categoriza los sistemas de IA en cuatro niveles básicos**:

- **Sistemas de IA inaceptables**: aplicaciones con potencial para vulnerar derechos fundamentales. Se incluyen tecnologías de manipulación cognitiva, sistemas de puntuación social y herramientas de reconocimiento facial en espacios públicos.

- **Sistemas de IA de alto riesgo**: abarcan sectores críticos como infraestructuras esenciales, educación, servicios bancarios y seguros. Estos sistemas requieren evaluaciones de conformidad rigurosas, documentación exhaustiva y supervisión humana continua.

- **Sistemas de IA de riesgo limitado**: deben cumplir obligaciones específicas de transparencia, informando claramente a los usuarios que están interactuando con un sistema automatizado.

- **Sistemas de IA de riesgo mínimo**: la mayoría de aplicaciones de IA se incluyen en esta categoría y se pueden utilizar libremente, aunque se fomentan códigos de conducta voluntarios.

¿Cómo funciona la norma ISO 42001 para la gestión de IA?

La norma ISO 42001 establece los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión de inteligencia artificial (SGIA). **Este estándar se fundamenta en cinco pilares esenciales**:

Procedimiento de comunicación interna y externa ISO 9001

En la gestión de la calidad, la **comunicación eficaz** es mucho más que un intercambio de mensajes: es un factor estratégico que asegura la alineación de los procesos, la cooperación interna y la confianza con los grupos de interés externos. Por este motivo, la norma **ISO 9001:2015** dedica un espacio específico a este aspecto en su cláusula 7, dentro de los requisitos de soporte.

El **procedimiento de comunicación interna y externa ISO 9001** establece cómo debe gestionarse la información relevante en una organización, definiendo no solo qué se comunica, sino también **cuándo, a quién, cómo y quién es responsable de transmitirla**. En este artículo analizaremos los elementos clave de este requisito, su importancia en la implementación de un **Sistema de Gestión de la Calidad** (SGC) y cómo las organizaciones pueden aplicarlo de manera práctica.

La comunicación como soporte en ISO 9001:2015

En la versión 2015 de la norma, la comunicación gana protagonismo respecto a ediciones anteriores. Ya no se trata únicamente de garantizar la circulación de información dentro de la organización, sino de **estructurar la comunicación como un proceso planificado** que impacta tanto en el ámbito interno como en el externo.

Esto significa que la empresa debe **determinar las comunicaciones necesarias para el SGC**, abarcando desde el personal operativo hasta clientes, proveedores, accionistas y otros grupos de interés. El objetivo es asegurar que la información fluya de forma adecuada para garantizar la **eficacia del sistema** y, en última instancia, la satisfacción del cliente.

Elementos clave en el procedimiento de comunicación

La norma ISO 9001 plantea cinco cuestiones básicas que toda organización debe responder al diseñar su plan o procedimiento de comunicación:

01. **Qué comunicar:** pueden ser resultados de auditorías, indicadores de desempeño, no conformidades, cambios en los procesos o cualquier información relevante para la calidad.

02. **Cuándo comunicar:** la periodicidad puede variar según el tipo de información; por ejemplo, reportes mensuales internos o notificaciones inmediatas a clientes ante incidencias.

03. **A quién comunicar:** público objetivo interno (empleados, directivos) o externo (clientes, proveedores, socios, administraciones).

Actualización de la norma ISO 14001:2026: ¿qué cambios se esperan y cómo prepararse?

La **actualización de la norma ISO 14001:2026** representa una evolución significativa en la gestión ambiental de las organizaciones. Esta nueva versión de **ISO 14001**, prevista para febrero de 2026, incorpora las tendencias globales más relevantes en sostenibilidad, digitalización y gestión de riesgos ambientales.

Esta actualización no solo mantiene la estructura de alto nivel común a las normas ISO, sino que **profundiza en aspectos críticos** como el cambio climático, la economía circular y la responsabilidad en la cadena de suministro. Tras ella, las organizaciones certificadas tendrán un periodo de transición de tres años para adaptarse a los nuevos requisitos.

Cronograma de la actualización de la norma ISO 14001:2026

Según **la hoja de ruta establecida**, el proceso de actualización de la norma ISO 14001:2026 sigue este calendario:

- **Febrero 2025**: publicación del proyecto de la norma internacional.
- **Febrero 2026** (previsible): lanzamiento oficial de ISO 14001:2026.
- **2026-2029**: periodo de transición de tres años para las organizaciones ya certificadas.

Las organizaciones que ya cuentan con la **certificación de la norma ISO 14001** deberán migrar sus sistemas antes del vencimiento del periodo de transición. Los organismos de certificación y el Foro Internacional de Acreditación serán quienes determinen las fechas específicas para completar esta transición.

¿Qué cambios principales incluye la actualización de la norma ISO 14001:2026?

Las novedades de que incorpora la actualización de la norma ISO 14001:2026 se centran en diferentes cuestiones. Entre las más relevantes, se pueden destacar:

Enfoque ampliado en temas ambientales globales

La nueva versión **extiende significativamente el alcance de consideraciones ambientales**.

Implementación de la norma ISO 42001: desafíos comunes y guía paso a paso para superarlos

La adopción masiva de sistemas de inteligencia artificial ha transformado el panorama empresarial. En este contexto, la **implementación de la norma ISO 42001** se ha convertido en una necesidad estratégica para aquellas organizaciones que buscan gestionar sus sistemas de IA con responsabilidad. Esta norma establece un marco integral de gobernanza que permite mitigar riesgos y maximizar beneficios.

Sin embargo, implementar un estándar tan novedoso también presenta desafíos que requieren una planificación precisa y recursos específicos. **Las organizaciones deben afrontar barreras técnicas, culturales y económicas** que pueden comprometer el éxito del proyecto. Comprender estos obstáculos y disponer de una metodología estructurada resulta fundamental para que la implementación de la norma ISO 42001 resulte exitosa.

Principales desafíos en la implementación de la norma ISO 42001

Los obstáculos son variados, pero identificarlos es fundamental para que las organizaciones puedan prepararse adecuadamente y desarrollar estrategias de mitigación efectivas.

- **Recursos y presupuesto limitados**

La implementación de la norma ISO 42001 implica una inversión. Pero los costes no derivan únicamente de la necesaria adaptación para cumplir los **requisitos del estándar**. El tiempo dedicado por los equipos de cumplimiento también genera gastos ocultos.

La falta de personal especializado agrava la situación. Los equipos de cumplimiento, ya sobrecargados en ocasiones con otros marcos normativos, deben asimilar conceptos técnicos complejos relacionados con IA. **Cualquier sobrecarga limita la capacidad de dedicar recursos suficientes a la implementación efectiva**.

- **Resistencia cultural al cambio**

La implementación de la norma ISO 42001 puede requerir ralentizar procesos de desarrollo para fortalecer las bases de la gobernanza. Esta filosofía entra en conflicto con culturas organizacionales enfocadas en velocidad y agilidad. **Los equipos técnicos pueden percibir el cumplimiento como un obstáculo que limita innovación** y competitividad.

Empresas con ISO 9001: ¿cuáles están certificadas?

Más de **un millón de organizaciones en todo el mundo** cuentan con la certificación ISO 9001, pero... **¿cómo saber cuáles están realmente certificadas en la práctica?** Encontrar a las **empresas con ISO 9001** implica revisar certificados, validar organismos acreditados y entender qué significa el alcance de cada certificación.

Lejos de ser un simple sello, la ISO 9001 es una herramienta que transforma la manera en que una empresa gestiona su calidad. Sin embargo, identificar a las compañías que cumplen con este estándar requiere un proceso de verificación y análisis más detallado de lo que se suele imaginar.

¿Qué significa estar certificado en ISO 9001?

La **ISO 9001** es la norma internacional que establece los requisitos para implementar un **Sistema de Gestión de la Calidad (SGC)**.

Cuando una organización obtiene el certificado, significa que un **organismo certificador acreditado** ha auditado sus procesos y ha comprobado que cumplen con estándares de calidad reconocidos a nivel global.

Esto garantiza que la empresa tiene definidos sus procesos, que mide y controla su desempeño y que está comprometida con la **mejora continua**. No obstante, hay que tener en cuenta que el certificado **no es indefinido**: requiere auditorías anuales de seguimiento y recertificación cada tres años, lo que asegura que el sistema se mantenga vigente.

¿Existe un listado único de empresas con ISO 9001?

Una de las primeras dudas que surge es si hay un directorio global con todas las organizaciones certificadas. La realidad es que **no existe un listado universal de empresas con ISO 9001**. Cada país y cada organismo certificador gestiona su propia base de datos.

Por tanto, si queremos comprobar si una empresa está certificada, debemos:

01. **Identificar con qué organismo certificador trabaja.**

02. **Acceder al buscador oficial del organismo** o solicitar información directamente.

03. **Revisar el certificado emitido**, verificando datos como vigencia, alcance y sedes incluidas.

De esta forma, evitamos aceptar información poco clara y nos aseguramos de que la empresa cumple realmente con la norma.

ISO 27001 y NIS 2: cómo se complementan y qué diferencias debes conocer

La relación entre **ISO 27001 y NIS 2** marca un punto de encuentro esencial entre la gestión voluntaria de la seguridad de la información y el cumplimiento normativo obligatorio. Ambos marcos, aunque diferentes en su naturaleza jurídica, comparten objetivos comunes que los convierten en aliados estratégicos para la ciberseguridad empresarial en el ámbito de la Unión Europea.

Comprender cómo se interrelacionan ISO 27001 y NIS 2 resulta esencial para aquellas organizaciones que buscan **optimizar la inversión en seguridad, alcanzar el cumplimiento y mejorar la resiliencia**. De hecho, la implementación coordinada de ambas normas puede generar importantes ventajas operativas y económicas.

¿Qué es la Directiva NIS 2?

La Directiva NIS 2 (Directiva sobre Seguridad de Redes y Sistemas de Información) entró en vigor en octubre de 2024, sustituyendo a la directiva NIS original de 2016. Esta evolución normativa **responde a la creciente sofisticación de las amenazas cibernéticas** y al mayor riesgo de **eventos de seguridad de la información**, además de a las limitaciones identificadas en su predecesora.

Su objetivo principal es **mejorar la protección de infraestructuras críticas** y armonizar las prácticas de seguridad en todos los estados miembros

Características principales de NIS 2

NIS 2, de carácter obligatorio, **se centra en 15 sectores clasificados en dos categorías**:

- **Sectores esenciales**: energía, transporte, finanzas, administración pública, salud, espacio, abastecimiento de agua e infraestructura digital.

- **Sectores importantes**: servicios postales, gestión de residuos, productos químicos, investigación, alimentación, fabricación y proveedores digitales.

Por otra parte, **la directiva introduce sanciones severas.** Las multas pueden alcanzar los 10 millones de euros o el 2% de la facturación global para entidades esenciales y 7 millones de euros o el 1,4% para entidades importantes.

Cumplimiento en IA: principales regulaciones y aplicación práctica

El **cumplimiento en IA** es requisito estratégico para las organizaciones que utilizan inteligencia artificial en sus procesos de negocio. Normas internacionales como **ISO 42001** han marcado un punto de inflexión, impulsando la necesidad de sistemas de gestión que aseguren transparencia, seguridad y ética en la aplicación de la inteligencia artificial.

El reto no consiste solo en cumplir con la regulación vigente, sino en **anticiparse a cambios normativos, gestionar los riesgos asociados y transformar la gobernanza digital** en una ventaja competitiva. Comprender esta realidad es clave para evitar sanciones, mejorar la gobernanza de datos y fortalecer la reputación empresarial.

Qué supone el cumplimiento en IA

El cumplimiento en IA es el proceso de garantizar que el desarrollo y uso de los sistemas de inteligencia artificial **respetan la**

normativa, los principios éticos y las obligaciones regulatorias aplicables. Se trata de un enfoque integral que combina políticas, controles, **gobernanza de la IA** y responsabilidad corporativa.

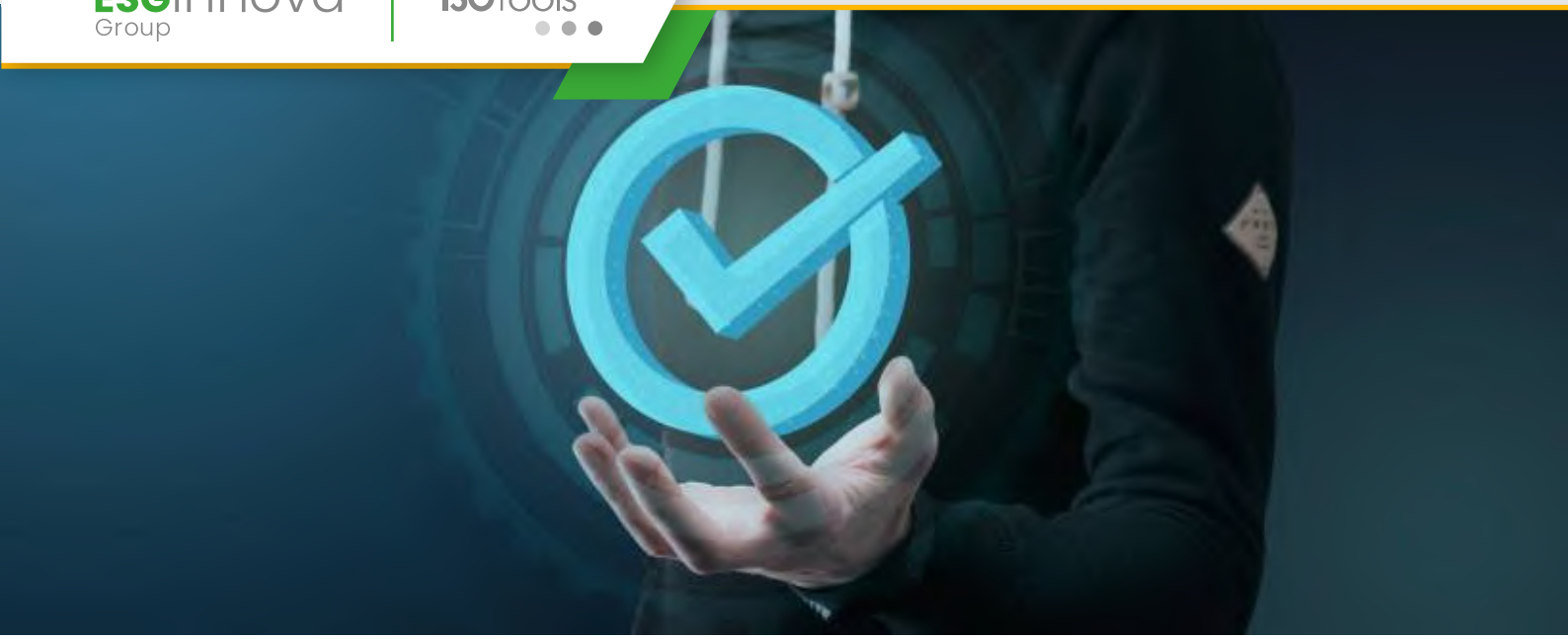
Los **ejes fundamentales** del cumplimiento en IA son cuatro:

- **Transparencia**: decisiones comprensibles y explicables para usuarios y auditores.
- **Seguridad**: medidas de protección para mitigar riesgos operativos, legales y reputacionales.
- **Equidad**: evitar sesgos en los datos de entrenamiento, en el diseño algorítmico y en los resultados, garantizando un impacto justo en todos los grupos sociales.
- **Responsabilidad**: designar roles claros para la supervisión y corrección de fallos, así como mecanismos de reclamación.

Estos principios no solo reducen riesgos legales y reputacionales, sino que también **construyen confianza en clientes, socios y otras partes interesadas**. Pero hay que tener en cuenta que su aplicación práctica exige revisar el diseño, implementación y supervisión de los sistemas de IA en todas sus fases de vida.

Regulaciones de IA: panorama internacional

Aunque la inteligencia artificial es una tecnología global, **su regulación avanza a distinta velocidad** según la región. Europa lidera este proceso, mientras que otros países optan por enfoques progresivos o voluntarios.



¿Qué significa UNE-EN ISO 9001 2015?

La **UNE-EN ISO 9001 2015** es una de las normas de gestión de calidad más reconocidas y utilizadas a nivel mundial. Representa la adaptación en España de la norma internacional **ISO 9001:2015**, integrando tanto el marco europeo (EN) como la referencia nacional (UNE). Este estándar establece los **requisitos mínimos para implementar un Sistema de Gestión de la Calidad (SGC)** que garantice que los productos y servicios cumplen con las expectativas de los clientes y con los requisitos legales y reglamentarios aplicables.

La certificación bajo UNE-EN ISO 9001 2015 no es obligatoria, pero sí constituye una herramienta estratégica para **mejorar procesos, aumentar la competitividad y fortalecer la confianza del mercado**. No en vano, se estima que en España más de **30.000 organizaciones ya cuentan con este certificado**, lo que la convierte en la norma de referencia para demostrar compromiso con la calidad.

¿Qué son las normas UNE-EN ISO?

Las **normas UNE-EN ISO** son el resultado de la adopción en España de estándares europeos (EN) e internacionales (ISO).

- **UNE (Una Norma Española):** es la denominación nacional, impulsada por la Asociación Española de Normalización (UNE), que representa a España en los organismos europeos e internacionales de normalización.

- **EN (European Norm):** indica que la norma ha sido aprobada en el ámbito europeo y debe ser adoptada por los estados miembros de la Unión Europea.

- **ISO (International Organization for Standardization):** hace referencia a la entidad internacional con sede en Ginebra que desarrolla normas reconocidas en más de 160 países.

De esta manera, la UNE-EN ISO 9001 2015 es la **versión española de la norma internacional ISO 9001:2015**, asegurando la coherencia de criterios en el marco nacional, europeo y global.

Principales requisitos de la UNE-EN ISO 9001 2015

La norma UNE-EN ISO 9001 2015 introduce un enfoque basado en **procesos y mejora continua**, alineado con el pensamiento basado en riesgos. Sus requisitos fundamentales incluyen:

- **Contexto de la organización:** identificar factores internos y externos que influyen en la gestión de la calidad.

Automatización de ISO 45001: impulsa la eficiencia en seguridad laboral con ISOTools

La **automatización de ISO 45001** marca un antes y un después en la gestión de seguridad y salud ocupacional. La digitalización de los procesos normativos no solo garantiza el cumplimiento regulatorio, sino que transforma radicalmente la eficiencia organizacional. En este contexto, la tecnología se convierte en una aliada cada vez más necesaria para construir entornos laborales más seguros, eficientes y sostenibles.

Los sistemas tradicionales de gestión manual muestran limitaciones críticas en la era digital. La complejidad creciente de las regulaciones laborales, combinada con la necesidad de respuesta inmediata ante incidentes, exige **soluciones tecnológicas avanzadas que permitan una gestión proactiva e inteligente** mediante la automatización de ISO 45001.

¿Qué es la norma ISO 45001?

La norma ISO 45001 es el **estándar internacional para sistemas de gestión de seguridad y salud en el trabajo**, publicada en marzo de 2018. Aunque su adopción no es obligatoria, proporciona un marco estructurado que mejora significativamente la seguridad laboral mediante un enfoque sistemático de **gestión de riesgos**.

La norma establece directrices para facilitar el diseño e implementación de políticas y **objetivos de seguridad** y salud específicos para cada empresa, **promoviendo una mentalidad preventiva y proactiva**. Su diseño permite la implementación en organizaciones de cualquier tamaño y sector.

Además, **proporciona metodologías para identificar y reducir riesgos de forma sistemática**, estableciendo procesos que permiten a los empleados informar sobre riesgos o incidentes. De esta manera se impulsa la mejora continua de la organización mediante el uso de datos y métricas.

¿Qué papel tiene la automatización de ISO 45001 en la gestión de seguridad laboral?

Gestionar ISO 45001 de forma manual implica limitaciones: retrasos en la información, errores humanos y dificultades en la trazabilidad documental, entre otras. Además, la falta de centralización de datos impide el análisis predictivo de riesgos.

La automatización de ISO 45001 permite superar estos obstáculos. Con un **software de gestión SST** es posible integrar y **centralizar datos procedentes de diferentes fuentes, realizar seguimientos en tiempo real y garantizar la mejora continua.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Auditoría ISO 42001: consejos prácticos basados en experiencias reales

La **auditoría ISO 42001** es un proceso clave para demostrar la madurez de una organización en la gestión responsable de la inteligencia artificial. Más allá de un requisito formal, supone una oportunidad estratégica para reforzar la confianza de clientes, socios y auditores, al validar que se han establecido marcos robustos para el desarrollo y uso ético de la IA.

Prepararse adecuadamente marca la diferencia entre superar la auditoría ISO 42001 con éxito o enfrentarse a hallazgos que pueden resultar costosos. Los que se enumeran a continuación son consejos prácticos resultado de la experiencia, una **hoja de ruta útil para organizaciones que buscan superar con éxito este proceso de evaluación** y **obtener la certificación** que demuestre su compromiso con la gestión responsable de la inteligencia artificial.

Involucrar al equipo: clave para afrontar una auditoría ISO 42001

El factor humano es el elemento determinante para superar una auditoría ISO 42001. Se requiere una preparación integral de los equipos que combine formación técnica con concienciación sobre la importancia estratégica de la norma.

Formación y concienciación

El primer paso hacia una auditoría ISO 42001 exitosa pasa por preparar adecuadamente a todos los actores involucrados. La capacitación implica **explicar los beneficios estratégicos de la norma**, no solo los **requisitos técnicos de ISO 42001**.

Es esencial que los equipos entiendan con claridad cómo la **gestión sistemática de la IA contribuye a mitigar riesgos**, mejorar la confianza del cliente y crear ventajas competitivas para la organización.

Comunicación y colaboración

Establecer canales de comunicación específicos es fundamental porque mantiene a todas las partes informadas sobre las actualizaciones en el proceso de auditoría. Esta transparencia **facilita la identificación temprana de obstáculos** y permite diseñar ajustes en la estrategia de implementación de ISO 42001.

Por otra parte, también es importante una colaboración estrecha entre departamentos tradicionalmente separados, como ingeniería y cumplimiento.

ISO 27005 vs ISO 31000: qué norma puede ayudarte más

En un contexto empresarial marcado por la **incertidumbre, la transformación digital y el aumento de los riesgos cibernéticos**, la **gestión de riesgos** se ha consolidado como un pilar estratégico para garantizar la continuidad de las operaciones y la confianza de los clientes. Sin embargo, surge una pregunta frecuente entre los profesionales: **¿ISO 27005 vs ISO 31000, cuál de estas normas es más útil para mi organización?**

Ambos estándares son reconocidos internacionalmente y ofrecen enfoques sólidos para abordar los riesgos, pero presentan diferencias significativas en su **alcance, propósito y nivel de especialización**. Mientras que la **ISO 27005** se centra en la **seguridad de la información**, la **ISO 31000** proporciona un marco general aplicable a cualquier tipo de riesgo.

ISO 27005: un enfoque en seguridad de la información

La **ISO 27005** es una norma que ofrece **directrices específicas para la gestión de riesgos de seguridad de la información**.

Está diseñada como complemento de la **ISO 27001**, y proporciona el marco metodológico para identificar, analizar y tratar los riesgos que afectan a la **confidencialidad, integridad y disponibilidad de la información**. Entre sus principales ventajas destacan:

- **Especialización**: aborda de forma concreta los riesgos de **ciberseguridad** y de **protección de datos**.
- **Integración natural con ISO 27001**: juntas, ambas normas conforman un **Sistema de Gestión de Seguridad de la Información (SGSI)** sólido.
- **Adaptabilidad**: se aplica a organizaciones de cualquier tamaño o sector que manejen información sensible o crítica.
- **Gestión proactiva de amenazas**: permite anticiparse a riesgos como accesos no autorizados, ataques de malware, fugas de información o interrupciones en la disponibilidad de sistemas.

En resumen, ISO 27005 es ideal para empresas cuya **prioridad es la protección de sus activos digitales** y que buscan una metodología alineada con las mejores prácticas internacionales de seguridad de la información.

ISO 31000: un marco de gestión de riesgos integral

La **ISO 31000**, por su parte, es un estándar internacional que establece **principios y directrices para la gestión de riesgos en cualquier ámbito organizacional**. No está limitada a la seguridad de la información, sino que puede aplicarse a riesgos financieros, estratégicos, legales, reputacionales, ambientales y operativos.

AI Act e ISO 42001: directrices de compatibilidad e implementación

La **convergencia entre la AI Act e ISO 42001** marca un punto de inflexión en la gestión responsable de sistemas de inteligencia artificial. Ambos marcos son pilares fundamentales para aquellas organizaciones que buscan implementar tecnologías de IA de manera ética y conforme a unas exigencias regulatorias en constante evolución.

Las organizaciones se enfrentan al reto de navegar por un escenario normativo complejo donde la conformidad legal y la excelencia técnica deben coexistir. La alineación entre AI Act e ISO 42001 ofrece una hoja de ruta para **alcanzar tanto el cumplimiento normativo como la certificación de calidad en la gestión de la inteligencia artificial**.

Diferencias entre AI Act e ISO 42001

La relación entre AI Act e ISO 42001 muestra puntos de encuentro estratégicos, pero también diferencias operativas fundamentales. Ambos marcos **persiguen garantizar el desarrollo e implementación segura de sistemas de IA**, pero abordan este objetivo desde perspectivas complementarias.

Enfoque y aplicación de la AI Act

La **Ley de Inteligencia Artificial de la UE** es el primer marco legal integral sobre inteligencia artificial aprobado en la Unión Europea. Su objetivo es **garantizar que los sistemas de IA sean seguros**, transparentes y respeten los derechos fundamentales.

Este reglamento **clasifica los sistemas de IA en cuatro niveles de riesgo**: inaceptable, alto, limitado y mínimo. Las organizaciones deben adaptar sus procesos según el nivel de riesgo, aplicando medidas como supervisión humana, documentación técnica y gestión de riesgos.

La AI Act **es una norma obligatoria** que se aplica a todas las organizaciones con operaciones en la Unión Europea. Su incumplimiento conlleva **sanciones económicas** significativas que pueden alcanzar hasta 35 millones de euros o el 7% del volumen de negocio anual global.

Enfoque y aplicación de ISO 42001

La norma ISO 42001 es el **estándar internacional para sistemas de gestión de inteligencia artificial**.

Software de gestión medioambiental: 7 requisitos clave para elegir la mejor solución para tu empresa

La sostenibilidad empresarial requiere herramientas especializadas que faciliten el cumplimiento normativo. Un **software de gestión medioambiental** se convierte así en un aliado estratégico necesario para optimizar procesos, reducir impactos ambientales y garantizar el cumplimiento de estándares internacionales como **ISO 14001**. La elección de la tecnología adecuada es clave en el éxito de la implementación del **sistema de gestión ambiental** (SGA). **No todas las soluciones digitales ofrecen las funcionalidades necesarias** para alcanzar objetivos ambientales críticos y mantener la competitividad empresarial en un mercado cada vez más exigente con la responsabilidad corporativa.

Qué criterios valorar para elegir el mejor software de gestión medioambiental

Para garantizar que la inversión tecnológica genere resultados tangibles, es imprescindible realizar un **análisis riguroso de los requisitos técnicos y funcionales** de las diferentes opciones. La elegida debe ser aquella en la que cada característica contribuya al cumplimiento normativo, a la optimización operativa y a la construcción de ventajas competitivas sostenibles.

Los siguientes requisitos constituyen los pilares fundamentales sobre los cuales se sustenta la implementación exitosa de una gestión ambiental automatizada.

1. Capacidades avanzadas de automatización de procesos

La **automatización del SGA** constituye la base de cualquier solución tecnológica eficaz. El software de gestión medioambiental **debe eliminar procesos manuales propensos a errores**, optimizar la recopilación de datos y garantizar la precisión en el análisis de información ambiental.

Una plataforma integral **automatiza la captura, procesamiento y análisis de datos** desde diversas fuentes. Esta centralización permite responder con rapidez a problemas emergentes y facilita ajustes proactivos en las estrategias ambientales. Todo ello se traduce en mayor eficiencia operativa.

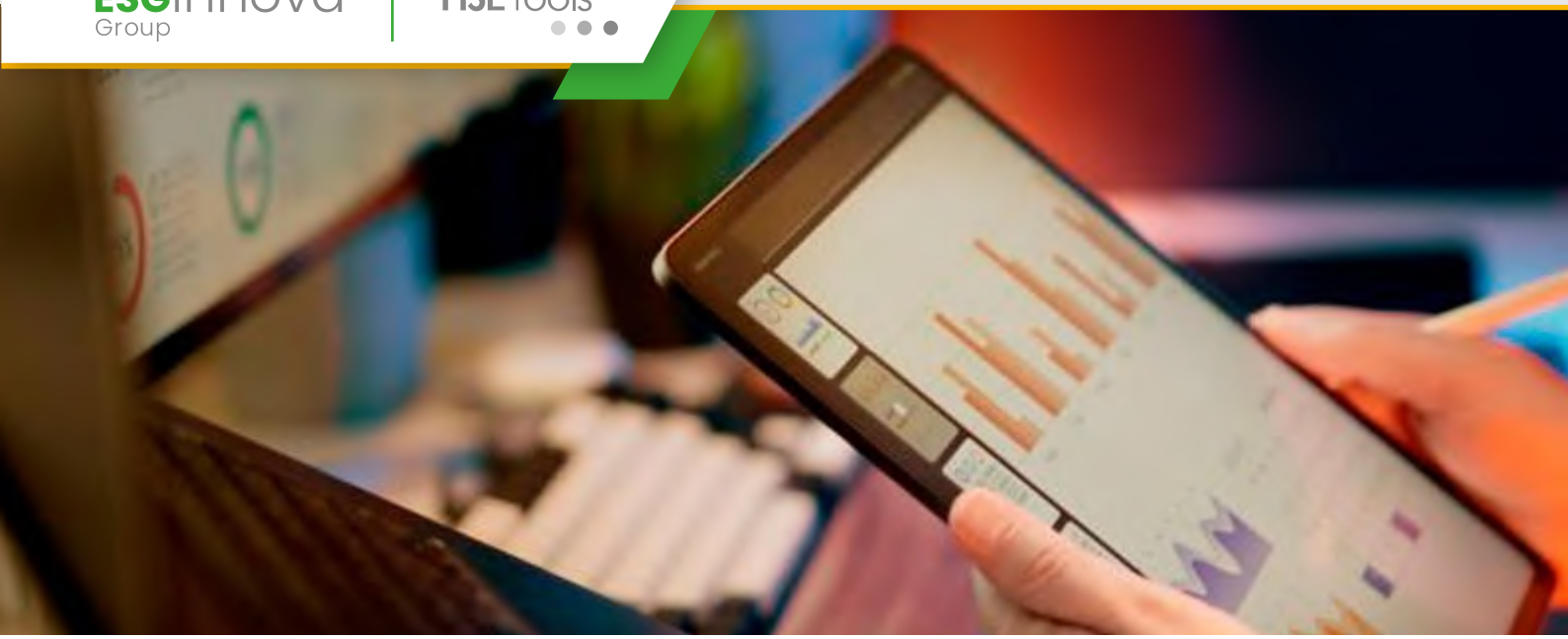
2. Garantía de cumplimiento normativo

El cumplimiento de normas y regulaciones diversas debe ser una funcionalidad nativa del software de gestión medioambiental elegido.

ESGinnova
Group

HSE Tools

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



Datos HSE centralizados: 5 formas en que el software mejora la seguridad y el cumplimiento

Los **datos HSE** componen el núcleo informativo de los programas de gestión de riesgos. Sin embargo, cuando estos datos críticos se encuentran dispersos en múltiples sistemas, formatos y departamentos, su potencial para mejorar la seguridad y garantizar el cumplimiento queda seriamente limitado. Una **gestión de documentos** eficiente resuelve esta problemática y elimina barreras para el acceso, análisis y utilización eficiente de la información.

La centralización de datos mediante un **software HSE** no es solo una mejora técnica, es una transformación estratégica. Permite a las organizaciones **pasar de un enfoque reactivo a uno proactivo en la gestión de riesgos**, el cumplimiento normativo y la mejora continua. Sin embargo, muchas organizaciones aún se apoyan en herramientas inadecuadas para tratar esa información.

El resultado es una gestión documental que obstaculiza la toma de decisiones, ralentiza las respuestas y genera vacíos de cumplimiento.

Principales desafíos en la gestión de datos HSE

La mayoría de las organizaciones generan ingentes cantidades de datos HSE: **informes de incidentes**, registros de formación, inspecciones de seguridad, auditorías ambientales, etc. Sin embargo, **la información puede acabar dispersa entre departamentos, almacenada en formatos incompatibles**, duplicada o en repositorios inaccesibles. Son cuestiones que generan retos importantes:

Pérdida de visión integral

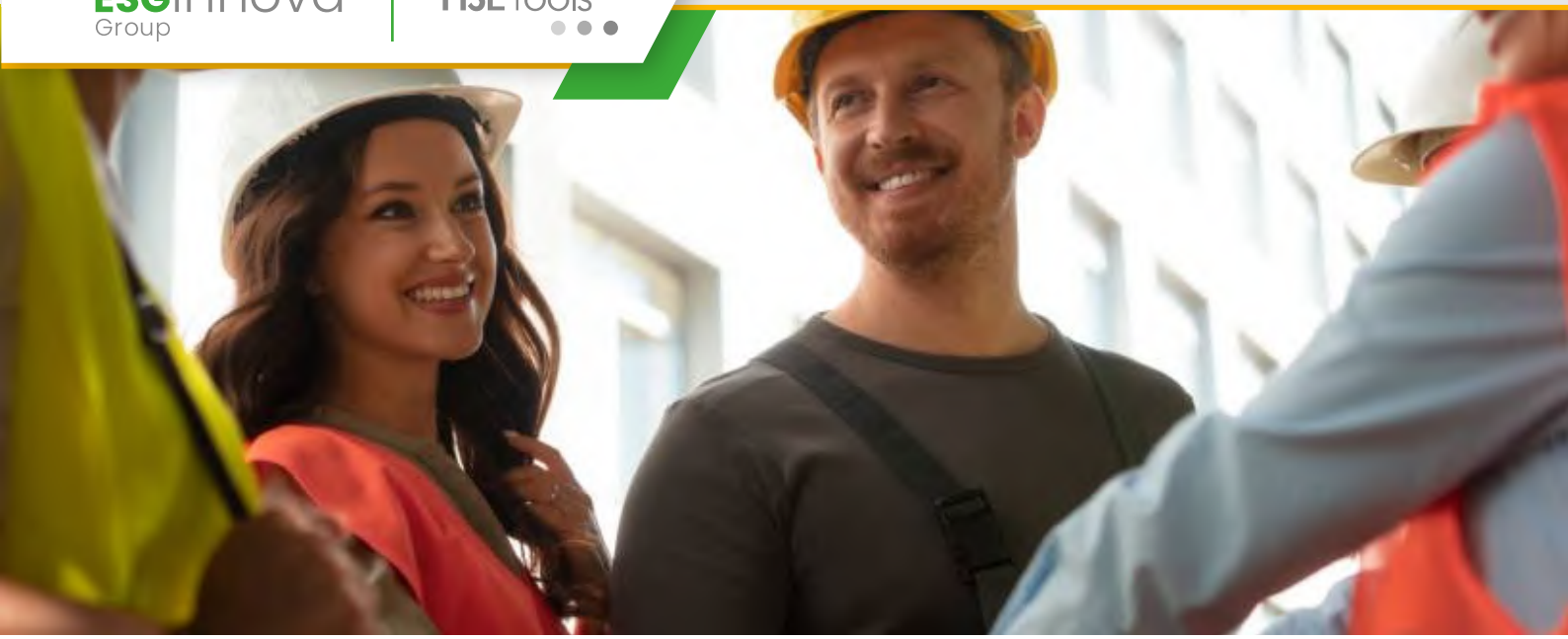
La fragmentación de la información o la falta de integración entre departamentos o herramientas provoca que los datos se dispersen. Esto impide una visión global, dificulta la detección de patrones y **genera decisiones basadas en datos parciales o inexactos**.

Retrasos en el acceso a los datos

Cuando la información se gestiona de **forma manual**, con formularios en papel, hojas de cálculo o correos, la revisión y el análisis se demoran. La consecuencia es que **resulta difícil actuar con celeridad**, especialmente en sectores críticos donde las condiciones cambian rápidamente y el tiempo de respuesta es vital.

Herramientas de reporte inadecuadas

Los informes manuales consumen tiempo y son propensos a errores.



Cómo aprovechar la cultura de seguridad para controlar los riegos de SST

La **seguridad y salud en el trabajo (SST)** constituye hoy uno de los pilares más estratégicos de cualquier organización. Ya no se trata únicamente de cumplir con las normas legales o evitar sanciones: la verdadera transformación ocurre cuando se construye una **cultura de seguridad** sólida, capaz de anticipar peligros y convertir la prevención en una práctica cotidiana. Este enfoque cambia el paradigma: de lo reactivo a lo preventivo, de lo impuesto a lo compartido.

A lo largo de este artículo revisaremos qué significa realmente cultura de seguridad, cómo impacta en el control de riesgos, cuáles son sus desafíos y qué papel juegan los líderes, los estándares internacionales y las nuevas herramientas digitales. Finalmente, mostraremos cómo una solución como **HSETools Gestión de Riesgos** puede servir como catalizador para convertir la cultura en resultados tangibles.

¿Qué entendemos por cultura de seguridad?

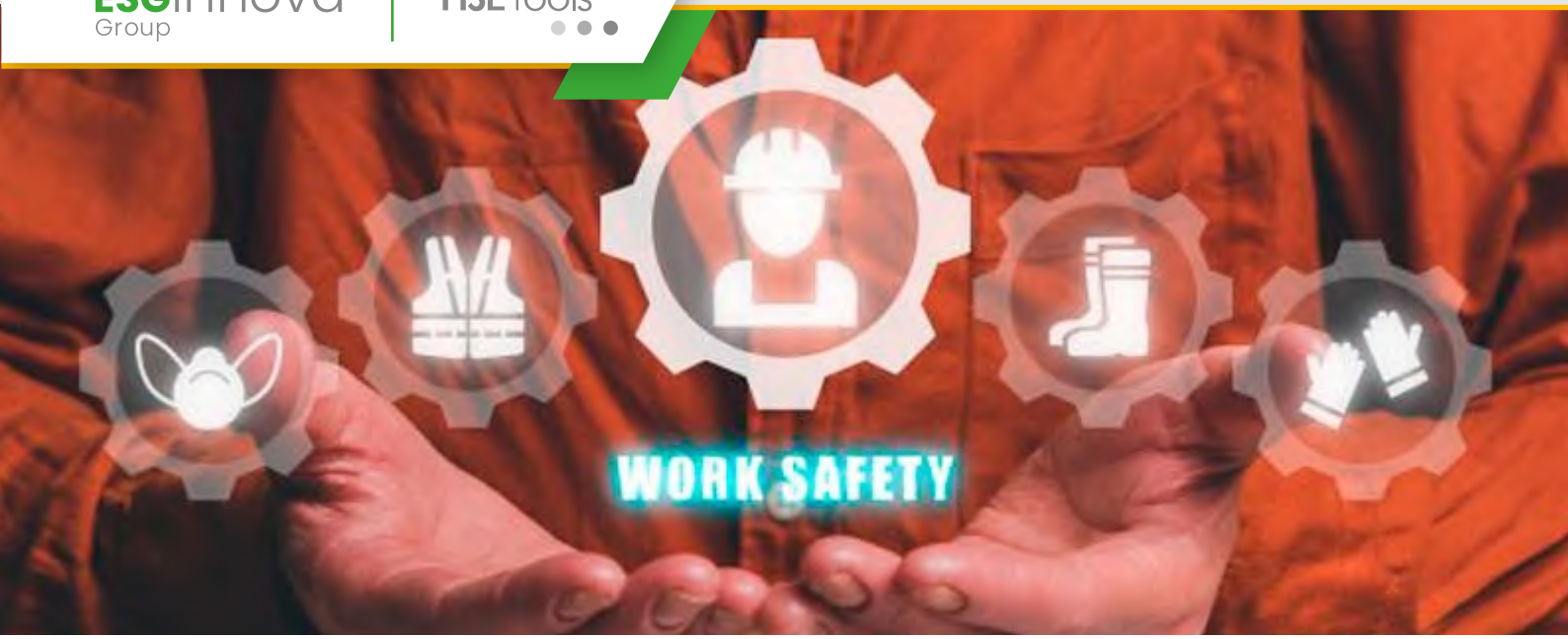
La **cultura de seguridad** no es un documento escrito ni un eslogan en la pared. Se trata de la forma en que los trabajadores piensan, sienten y actúan respecto a la seguridad en su día a día. Es la suma de actitudes, valores, comportamientos y prácticas que se manifiestan en los talleres, oficinas, plantas o faenas.

Cuando existe una cultura madura, los empleados cumplen las reglas porque comprenden su sentido, los supervisores lideran con coherencia y los directivos respaldan las decisiones preventivas aunque impliquen costes adicionales. Por el contrario, cuando la cultura es débil, surgen atajos peligrosos, se normalizan prácticas inseguras y los índices de accidentes se disparan.

De la cultura de seguridad al control de riesgos

El vínculo entre cultura de seguridad y **control de riesgos** es directo. Una cultura robusta actúa como una red invisible que **detecta y corrige desviaciones antes de que se conviertan en accidentes**. En entornos con alto riesgo operativo, la diferencia puede ser la vida de un trabajador o la continuidad de una planta.

Un ejemplo frecuente es la gestión de **riesgos ergonómicos**. Cuando los trabajadores están sensibilizados y reportan posturas forzadas o movimientos repetitivos, la organización puede rediseñar tareas, incorporar pausas activas o introducir ayudas mecánicas. De no existir esa cultura, los problemas pasan desapercibidos hasta que aparecen lesiones musculoesqueléticas, bajas prolongadas y altos costes asociados.



Crear un plan HSE integral: pasos clave y ejemplos

Para organizaciones de todo tipo, desarrollar un **plan HSE** se ha convertido en una prioridad estratégica que trasciende el simple cumplimiento normativo. Las empresas deben enfrentarse a presiones cada vez mayores para demostrar su compromiso con la seguridad laboral, la salud ocupacional y la protección ambiental, a la vez que mantienen su productividad y competitividad. En este escenario, los **planes de acción HSE** cobran protagonismo.

La implementación de un **sistema de gestión HSE** robusto no solo protege a trabajadores y medio ambiente. También **genera beneficios tangibles**: reducción de costes por accidentes, mejora de la reputación corporativa, cumplimiento regulatorio y aumento de la satisfacción de los empleados.

Claves de un plan HSE efectivo

Un plan HSE integral representa el marco estratégico que **define políticas, procedimientos y responsabilidades** para gestionar los riesgos de salud, seguridad y medio ambiente en una organización.

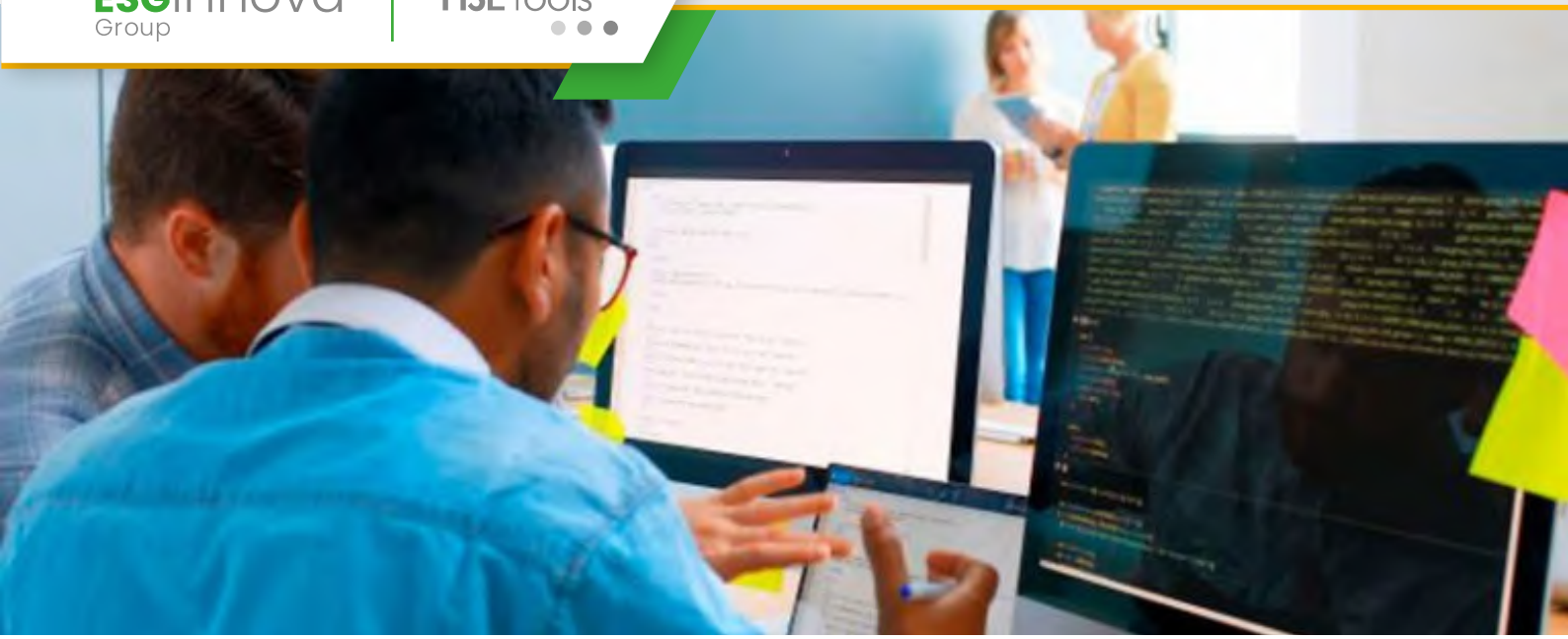
Es un documento dinámico que debe adaptarse constantemente a las necesidades específicas de la empresa y de los cambios normativos. Para ello, debe incluir toda una serie de componentes esenciales:

- **Declaración de compromiso**: es la manifestación clara de la alta dirección sobre la importancia de la gestión HSE.
- **Objetivos**: prevenir accidentes e incidentes laborales, cumplir con la legislación vigente en materia de HSE, minimizar impactos ambientales negativos, promover una **cultura de seguridad y salud** en todos los niveles de la organización, etc.
- **Estructura organizacional**: definición de responsabilidades desde la alta dirección hasta los trabajadores operativos, especificando claramente quién se encarga de qué.
- **Procedimientos operativos**: protocolos específicos para cada actividad de riesgo o medidas de control para mitigar los riesgos identificados durante la evaluación, entre otros.
- **Sistemas de monitoreo**: métricas e indicadores para evaluar el desempeño.
- **Planes de emergencia**: protocolos de respuesta ante incidentes y crisis (rutas de evacuación, contactos de emergencia, etc.).

Paso a paso: cómo implementar un plan HSE

Diseñar e implementar un plan HSE es **un proceso estructurado en el que cada fase es crítica**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Software de seguridad en el trabajo: cómo elegir la mejor opción según funcionalidad, coste y valor

Para las organizaciones modernas, el **software de seguridad en el trabajo** se ha convertido en herramienta clave para alcanzar el objetivo de una **gestión HSE preventiva** eficaz. La digitalización de los procesos de prevención no solo responde a una tendencia motivada por los avances tecnológicos, sino que representa una necesidad para optimizar recursos, garantizar el cumplimiento normativo y reducir los riesgos operacionales.

Las organizaciones que integran soluciones tecnológicas avanzadas en sus sistemas de prevención avanzan en la **mejora de indicadores clave como la reducción de accidentes laborales**, el cumplimiento de auditorías y la optimización de costes operativos.

La **transformación digital**, por otra parte, permite a los responsables de HSE enfocar sus esfuerzos en actividades estratégicas de alto valor, dejando a un lado tareas administrativas repetitivas que consumen recursos.

¿Por qué un software de seguridad en el trabajo es tan importante?

Un sistema de gestión de seguridad en el trabajo bien diseñado **actúa como columna vertebral de cualquier programa de prevención eficiente**. No solo permite cumplir con la normativa vigente, sino que **ayuda a identificar, evaluar y mitigar riesgos**. Así, las organizaciones que invierten en tecnología de gestión de seguridad pueden aprovecharse de ventajas significativas.

Cumplimiento normativo proactivo

El marco regulatorio en materia de **prevención de riesgos laborales** es complejo y está en constante evolución. Para las organizaciones, esto implica la necesidad de contar con **sistemas capaces de adaptarse a los cambios normativos** y responder a requisitos cada vez más específicos respecto a documentación, trazabilidad y presentación de informes. Requisitos que es inviable gestionar con eficacia mediante procesos manuales. **Un software de seguridad en el trabajo es capaz de automatizar acciones** como seguimiento de obligaciones legales, generación de informes y mantenimiento de registros actualizados. Esta capacidad resulta especialmente útil para enfrentarse con éxito a auditorías e inspecciones, procesos en los que la presentación organizada y completa de la documentación puede determinar el resultado.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cumplimiento de proveedores y contratistas: mejores prácticas para estandarizar y centralizar la gestión

El **cumplimiento de proveedores** y de terceros en general es un aspecto crítico a la hora de garantizar la seguridad, eficiencia y continuidad operativa de las organizaciones. La **gestión de contratistas** no es una tarea administrativa, sino un proceso estratégico que involucra la verificación de credenciales, el seguimiento documental y el mantenimiento de estándares de seguridad en todos los niveles de la cadena de suministro. En ese escenario, la tecnología y la automatización se posicionan como aliados indispensables.

La creciente complejidad del panorama normativo, unido a la dispersión geográfica cada vez mayor de las operaciones, hacen que las organizaciones que trabajan con terceros se enfrenten a **riesgos legales, operativos y reputacionales si no establecen mecanismos sólidos** para verificar que todos sus

colaboradores externos cumplen con los requisitos normativos, de seguridad y de calidad.

Principales desafíos relacionados con el cumplimiento de proveedores

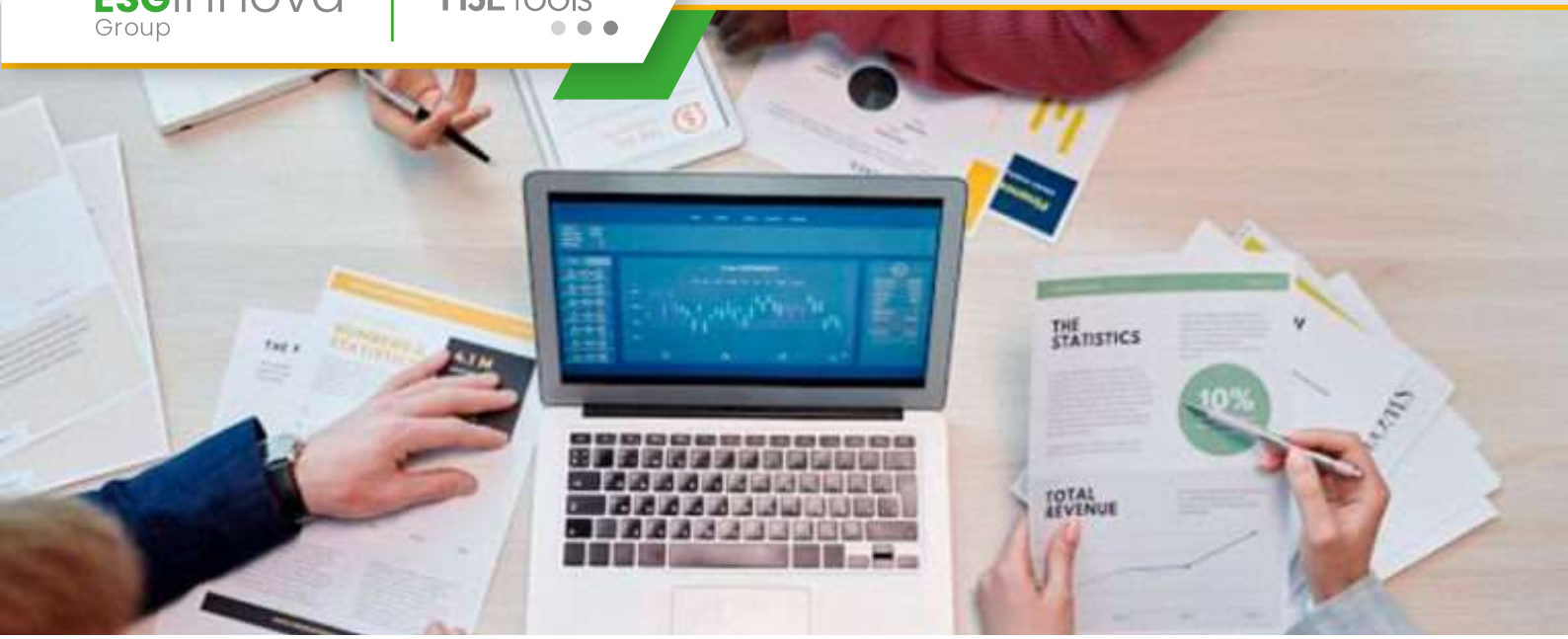
Gestionar terceros implica más que recopilar documentos o validar licencias. Entre los **desafíos comunes en la gestión de contratistas** y proveedores cabe destacar los siguientes:

Fragmentación de la información

Una de las principales dificultades en la gestión tradicional de terceros radica en la **dispersión de datos críticos**. Las organizaciones suelen conservar la información de proveedores en múltiples sistemas, desde hojas de cálculo a archivos físicos o correos electrónicos. Esta fragmentación genera ineficiencias operativas y aumenta el riesgo de un cumplimiento de proveedores ineficaz. La falta de centralización dificulta el seguimiento de vencimientos documentales, la verificación de credenciales actualizadas y una **evaluación de proveedores** integral. Además, **complica la trazabilidad de procesos** durante auditorías internas o inspecciones regulatorias.

Procesos manuales y redundantes

Los métodos tradicionales de gestión dependen excesivamente de procesos manuales que consumen tiempo y recursos. **La revisión documental, el seguimiento de renovaciones y la comunicación de requisitos se realizan de forma reactiva**, generando retrasos en la incorporación de nuevos proveedores y potenciales interrupciones en los proyectos.



Aplicación HSE: guía práctica para elegir el software de gestión ambiental, salud y seguridad

La transformación digital ha revolucionado la gestión empresarial en todos los sectores y el ámbito de la seguridad, salud y medio ambiente no es una excepción. En este contexto, trabajar con una **aplicación HSE** es fundamental para las organizaciones que buscan optimizar sus procesos de **gestión de documentos**, mejorar sus planes de acción en la materia y garantizar el cumplimiento normativo.

La implementación de soluciones digitales especializadas no solo mejora la eficiencia operativa, sino que también fortalece la **cultura de seguridad** y reduce significativamente los riesgos asociados a la actividad empresarial. La selección de la aplicación HSE adecuada es **una decisión estratégica que impacta en el desempeño de la organización**, pero es imprescindible identificar correctamente qué solución se adapta mejor a sus necesidades específicas.

Esta guía práctica pretende proporcionar los **criterios esenciales para evaluar y seleccionar la aplicación HSE** más adecuada en cada caso. Para ello, es necesario evaluar aspectos muy diferentes que se detallan a continuación.

1. Alineación con las necesidades específicas de la organización

Análisis de requerimientos funcionales

El primer paso es realizar un **diagnóstico profundo de los desafíos HSE específicos de la organización**. Cada sector productivo presenta particularidades que requieren funcionalidades especializadas. Por ejemplo, la industria química demanda capacidades avanzadas de gestión de sustancias peligrosas, mientras que la construcción necesita herramientas sólidas para la **gestión de contratistas**. **La escalabilidad es otro factor clave**. La aplicación HSE debe crecer junto con la organización, adaptándose a nuevas ubicaciones, incremento de usuarios o expansión de unidades de negocio.

Personalización y configurabilidad

Una aplicación HSE efectiva debe **permitir la personalización de formularios, flujos de trabajo y reportes** según los procedimientos internos de la organización. La capacidad de configurar indicadores específicos y adaptar la terminología a su contexto marca la diferencia entre una herramienta genérica y una solución verdaderamente útil.

Gestión documental CAE: cómo asegurar el cumplimiento normativo de los contratistas

El cumplimiento normativo es prioritario en la **gestión de contratistas**. En ese camino, la **gestión documental CAE** (Coordinación de Actividades Empresariales) no es solo un requisito legal, es también pieza clave para garantizar la seguridad, la eficiencia y la reputación corporativa. No solo implica el control de documentación, sino la implementación de sistemas que aseguren la trazabilidad, actualización y verificación continua de credenciales críticas.

En un entorno en el que la fuerza laboral externa tiene una enorme relevancia, muchas organizaciones se enfrentan al desafío de manejar grandes volúmenes de documentación dispersa. **Las consecuencias de una gestión documental CAE deficiente pueden ser devastadoras**: desde sanciones regulatorias hasta incidentes que comprometan la seguridad laboral y la reputación corporativa. **Una metodología sólida y soluciones tecnológicas**

avanzadas resultan fundamentales para centralizar, automatizar y supervisar los procesos de manera ágil. Se reducen así riesgos, se consigue el **cumplimiento de proveedores y contratistas** y se optimizan recursos.

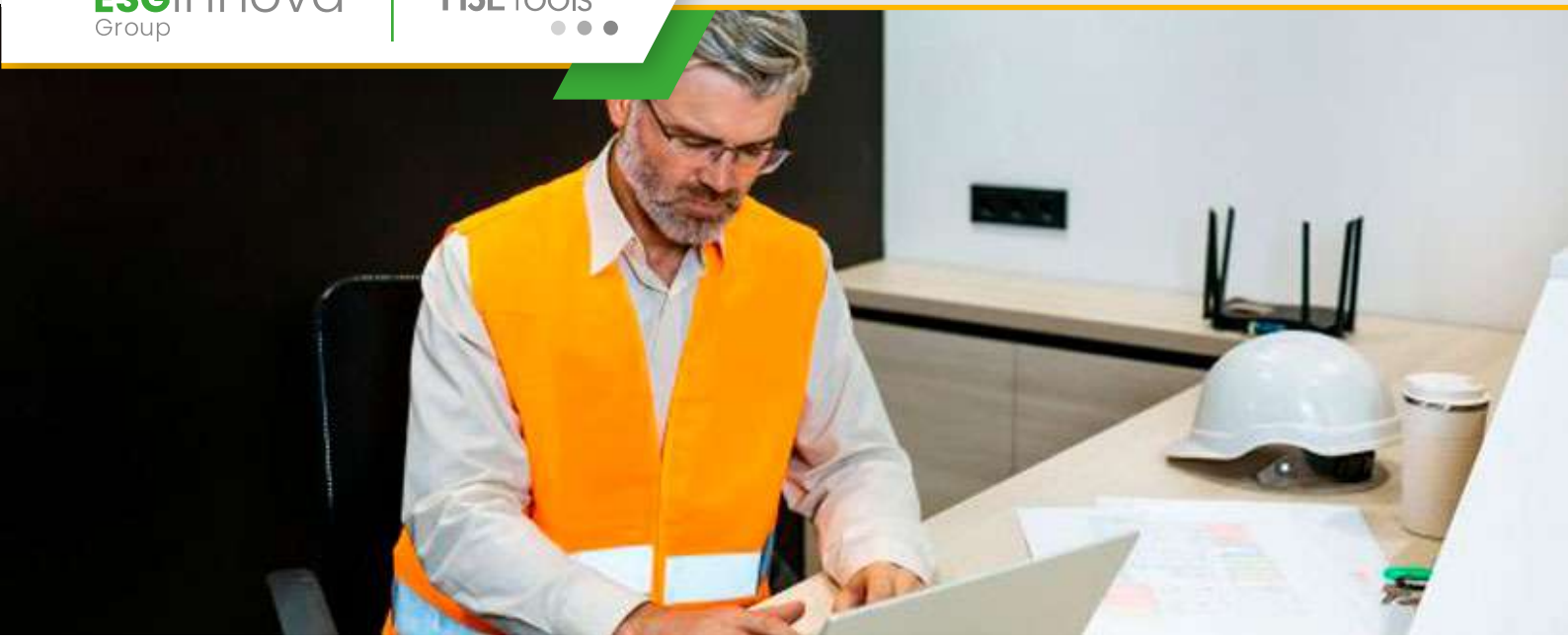
Qué es la gestión documental CAE

La gestión documental CAE es el **conjunto de procesos sistemáticos destinados a controlar, organizar y verificar la documentación necesaria** para el cumplimiento normativo en la coordinación de actividades empresariales. Incluye desde certificaciones de seguridad y pólizas de seguros hasta licencias profesionales y registros de formación. A diferencia de la gestión documental tradicional, la gestión documental CAE **requiere un enfoque especializado** que considere las particularidades del marco regulatorio HSE. El objetivo principal es garantizar que contratistas y colaboradores externos mantengan sus credenciales vigentes y cumplan con los requisitos establecidos por la organización contratante. **Normas internacionales como ISO 45001 establecen requisitos específicos para la gestión de contratistas**, exigiendo que las organizaciones implementen controles documentales sólidos que aseguren la competencia y autorización de terceros que operan en sus instalaciones.

Principales desafíos de la gestión documental CAE

La gestión documental CAE no está exenta de retos. Entre los más significativos, cabe destacar los siguientes:

- **Dispersión de la información en múltiples ubicaciones**: genera riesgos como pérdida de documentos, duplicidad de registros, dificultades para localizar información y falta de visibilidad sobre el estado real del cumplimiento.



Software de Gestión de Incidencias moderno: 7 razones para implementarlo en tu empresa

Un **Software de Gestión de Incidencias** es una herramienta imprescindible para organizaciones que buscan profesionalizar su enfoque en la **gestión de accidentes e incidentes**. Ya no basta con reaccionar ante un evento, es necesario disponer de sistemas digitales que permitan actuar de manera proactiva, documentar cada paso y asegurar la mejora continua en sus procesos de seguridad y salud en el trabajo.

Una solución digital especializada es básica en la capacidad de una empresa para **anticiparse a los riesgos y mantener la continuidad operacional**. Permite centralizar la información, automatizar **flujos de trabajo HSE** y proporcionar análisis predictivos para identificar patrones de riesgo antes de que se materialicen en accidentes. Esta evolución tecnológica representa una ventaja competitiva decisiva para organizaciones comprometidas con una cultura de seguridad sólida.

Desafíos de la gestión tradicional de incidencias

A diferencia de un Software de Gestión de Incidencias, **los sistemas tradicionales de gestión muestran limitaciones estructurales** que pueden comprometer la eficacia organizacional. Estas deficiencias no solo afectan la capacidad de respuesta inmediata, sino que obstaculizan el desarrollo de estrategias preventivas sostenibles.

Limitaciones de los procesos manuales

Los **métodos de gestión de seguridad laboral manuales** presentan deficiencias que comprometen la eficacia operacional. La documentación en papel genera **retrasos significativos en el procesamiento de información crítica**, mientras que la dispersión de datos en diferentes sistemas dificulta el análisis integral de tendencias. La falta de estandarización en los procesos de registro provoca **inconsistencias que obstaculizan la identificación de causas raíz**. Y, en este escenario, los equipos de seguridad tienen dificultades para obtener visibilidad completa sobre el estado de las investigaciones y el seguimiento de acciones correctivas.

Impacto en la cultura de seguridad

La gestión manual genera barreras que desincentivan el reporte de incidencias. Los empleados perciben los procesos burocráticos como obstáculos, lo que provoca que no se notifiquen **cuasi accidentes** y observaciones de seguridad. Esta situación impide que las organizaciones desarrollen estrategias preventivas basadas en datos completos y precisos.

¿Por qué los procedimientos de seguridad no siempre conducen a conductas seguras?

En teoría, los **procedimientos de seguridad** existen para proteger a los trabajadores y garantizar que las tareas se realicen sin riesgos. Cada paso está diseñado para prevenir **incidentes**, minimizar la exposición a peligros y cumplir con normativas. Sin embargo, la realidad demuestra que, en muchos casos, **tener procedimientos no asegura que se traduzcan en comportamientos seguros**.

¿Por qué ocurre esto? ¿Qué lleva a que en entornos con manuales, protocolos y capacitaciones siga habiendo accidentes graves? La respuesta no siempre está en los trabajadores, sino en el **entorno cultural y organizacional** que rodea su día a día.

Procedimientos de seguridad: Necesarios pero no suficientes

Cuando ocurre un incidente, la primera pregunta suele ser: "¿se siguieron los procedimientos?". Si la respuesta es negativa, se concluye que el problema está en la conducta del trabajador. Pero esta visión es limitada.

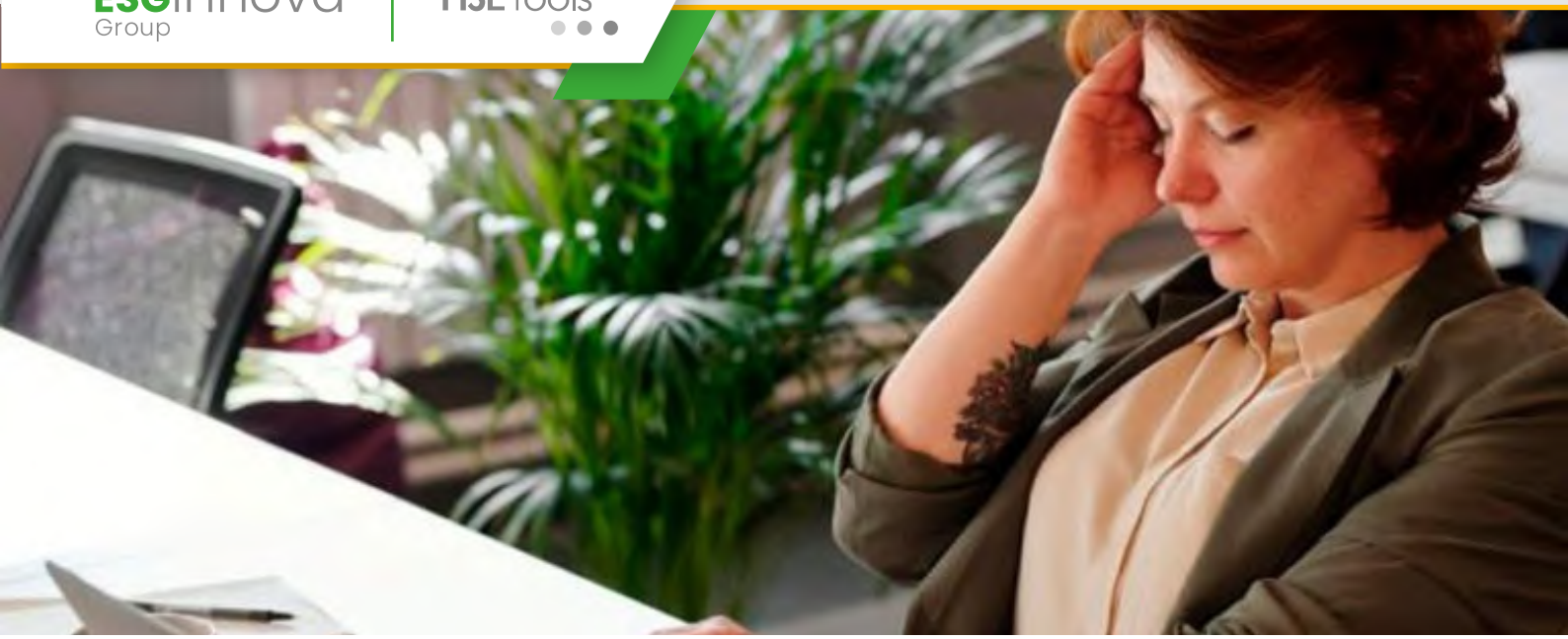
En muchos casos, los **procedimientos de seguridad** son demasiado complejos, consumen tiempo excesivo o resultan poco prácticos. Con el paso del tiempo, el equipo normaliza "atajos" o maneras alternativas de hacer el trabajo, generando lo que se conoce como **normalización de la desviación**: se crea una nueva "normalidad" en la que las prácticas inseguras se vuelven aceptadas mientras no haya incidentes visibles.

La ausencia de accidentes, sin embargo, no significa ausencia de riesgo. La cultura organizacional puede estar incubando el terreno para un desastre sin que nadie lo advierta.

El rol de la cultura en la seguridad

La seguridad no depende solo de lo que está escrito en un manual, sino de la **cultura de la organización**. Factores como la comunicación, la confianza o la manera en que los líderes reaccionan ante las desviaciones marcan la diferencia.

Si los trabajadores sienten que no pueden hablar abiertamente de problemas, pedir ayuda o cuestionar un procedimiento sin sufrir consecuencias negativas, es probable que opten por el silencio. Y esa falta de comunicación ascendente puede costar vidas.



Fatiga laboral y salud mental: cómo gestionarlas para mejorar la seguridad en el trabajo

La **fatiga laboral** y los problemas de salud mental representan uno de los mayores retos para los responsables del área de Seguridad y Salud en el Trabajo (SST). Son factores críticos para la seguridad, la eficiencia y la productividad de las organizaciones. La gestión efectiva de estos riesgos requiere sistemas integrados de **vigilancia de la salud** que identifiquen de forma temprana los indicadores de desgaste físico y mental en los trabajadores y permitan anticipar riesgos.

Aquellas organizaciones que implementan **estrategias proactivas para abordar la fatiga laboral y tratar los problemas de salud mental no solo mejoran sus indicadores de seguridad**. También optimizan el rendimiento operativo y reducen costes asociados a **ausentismo laboral**, rotación de personal y compensaciones por accidentes laborales.

¿Cuál es el impacto de la fatiga laboral?

La fatiga laboral tiene **consecuencias personales, pero también operacionales**. Entre las más relevantes, se encuentran las siguientes:

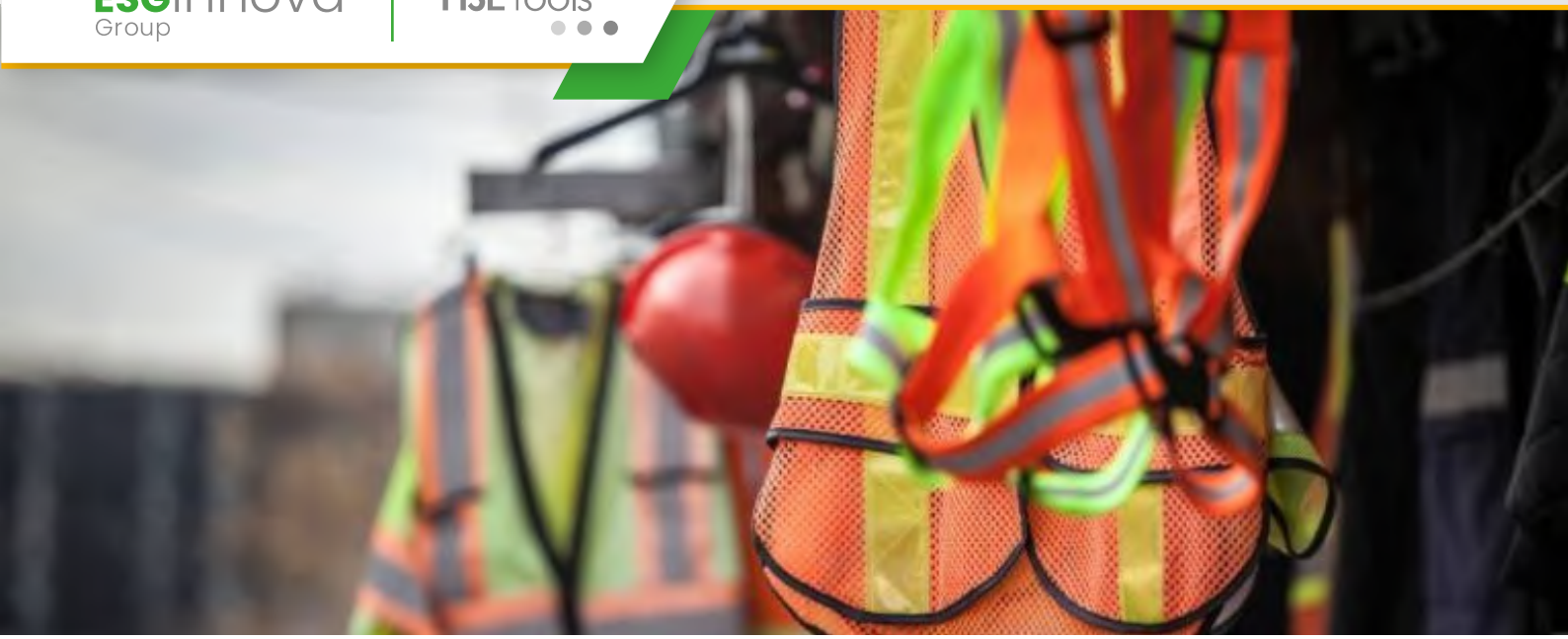
- **Deterioro de los procesos de seguridad**: trabajadores fatigados tienden a omitir protocolos, acelerar procedimientos críticos o saltarse controles rutinarios, incrementando el riesgo de incidentes graves.

- **Reducción de la percepción de riesgos**: la fatiga laboral disminuye la concentración y la conciencia situacional, provocando que los trabajadores subestimen la gravedad de los peligros o los ignoren.

- **Pérdida de capacidad de respuesta**: el procesamiento de información se ralentiza. Un retraso de apenas un segundo puede determinar la diferencia entre prevenir un accidente y una lesión grave.

- **Deterioro de la comunicación**: los empleados física o mentalmente sobrecargados malinterpretan instrucciones, olvidan detalles cruciales o no comunican anomalías, alterando los sistemas de seguridad.

De esta forma, no prevenir el **cansancio en el lugar de trabajo** se traduce en riesgos críticos: **mayor número de accidentes, lesiones más graves**, incremento de las bajas laborales y de los costes por indemnizaciones y pérdida de productividad.



Teoría del empujón para cumplir con las normas sobre EPP

El cumplimiento de las **normas sobre EPP (Equipos de Protección Personal)** es un desafío recurrente en la mayoría de las industrias. Aunque existen protocolos claros y las consecuencias de no respetarlos son bien conocidas, muchas organizaciones siguen enfrentándose a la resistencia de los trabajadores para usar de manera adecuada cascos, guantes, gafas o calzado de seguridad.

¿Por qué ocurre esto? La respuesta está en la **naturaleza humana**: las personas tienden a priorizar la comodidad inmediata sobre la seguridad a largo plazo. Es aquí donde la **teoría del empujón (Nudge Theory)** ofrece un enfoque innovador. En lugar de imponer controles rígidos o sanciones severas, esta teoría propone **pequeños cambios en el entorno que orienten la conducta hacia el uso seguro del EPP**, de forma natural y casi automática.

¿Qué es la teoría del empujón relacionada con las normas sobre EPP?

La **Nudge Theory** nace de la economía conductual y se centra en cómo la manera en que se presentan las opciones influye en nuestras decisiones. No se trata de prohibir ni de obligar, sino de diseñar el entorno para que la opción más segura sea también la más fácil y atractiva.

Aplicada a la seguridad laboral, esta teoría busca que el cumplimiento de las **normas sobre EPP** no dependa solo de la disciplina individual, sino de un contexto que facilite la decisión correcta. Dicho de otro modo: que ponerse el EPP se convierta en el camino natural, en lugar de un esfuerzo extra.

Cómo aplicar la teoría del empujón en el uso del EPP

Existen varias estrategias prácticas que muestran cómo los nudges pueden aumentar significativamente el cumplimiento:

Señales visuales simples y efectivas en las normas sobre EPP

Un cartel llamativo con el mensaje **"¿Llevas tus guantes?"** colocado justo en la entrada de un área crítica actúa como recordatorio inmediato. Lo importante es que el mensaje sea claro, visual y memorable.

Accesibilidad del EPP

Si el equipo de protección está disponible en puntos estratégicos de alto tránsito, los trabajadores tenderán a utilizarlo con mayor frecuencia. Colocar dispensadores junto a la maquinaria o casilleros en la entrada elimina barreras innecesarias.

Gestión documental en seguridad laboral: claves para un sistema de prevención eficaz

La **gestión documental en seguridad laboral** es una cuestión crítica para muchas organizaciones. La dispersión de la información, políticas disgregadas en diferentes versiones, instrucciones desactualizadas o registros que no están vinculados a riesgos y controles ralentizan la toma de decisiones y comprometen el cumplimiento. En este escenario, una adecuada **gestión de documentos y registros** aporta evidencia, coherencia y gobierno sobre una información que debe ser veraz, actualizada y accesible.

Los sistemas tradicionales de almacenamiento de la información han quedado obsoletos ante la **necesidad de gestionar volúmenes cada vez mayores de datos** en la gestión documental en seguridad laboral. La digitalización es la respuesta a ese reto.

Las áreas HSE necesitan sistemas integrados que permitan el acceso inmediato a la documentación actualizada, faciliten la colaboración entre departamentos y aseguren la trazabilidad completa de todos los procesos de seguridad a lo largo de su ciclo de vida.

Gestión documental en seguridad laboral: qué es y cuáles son sus componentes esenciales

Un **sistema de gestión de seguridad ocupacional** requiere una documentación perfectamente estructurada que abarque múltiples dimensiones organizativas. Es necesario tener en cuenta que la gestión documental en seguridad laboral **abarca desde la creación, aprobación y publicación de políticas SST a procedimientos, instrucciones**, permisos de trabajo o registros de incidentes, entre otros muchos elementos. Su misión es garantizar la integridad, disponibilidad y control de versiones, además de definir acceso y responsabilidades. Trata, en definitiva, de **convertir los documentos en la columna vertebral del sistema HSE**. Entre ellos, algunos son de enorme relevancia:

Política de salud y seguridad

El documento que reúne las **políticas SST define objetivos, responsabilidades y procedimientos en materia de seguridad laboral**. Su objetivo es sentar las bases de todas las actividades preventivas de la organización.

Debe ser un documento dinámico, que se adapte a los continuos cambios organizacionales, tecnológicos y normativos.

ESGinnova Group

GRCTools

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

3 factores claves para la seguridad de la información en la empresa

La **seguridad de la información en la empresa** no es un lujo ni una opción: es un pilar fundamental para garantizar la continuidad, la confianza de clientes y socios, y la competitividad a largo plazo. A medida que crece la digitalización —y con ella, amenazas como el phishing, ransomware y brechas de datos impulsadas por IA— proteger los activos de información se convierte en una prioridad estratégica. En este artículo analizamos **tres factores críticos** que aseguran una defensa eficiente y robusta.

1. Confidencialidad, integridad y disponibilidad: la tríada imprescindible

En la base de cualquier proyecto de **seguridad de la información**, se encuentra la reconocida **tríada CID**:

- **Confidencialidad**: asegurar que solo el personal autorizado tenga acceso a la información sensible.

- **Integridad**: garantizar que los datos no sean alterados de forma no autorizada, manteniendo su exactitud y consistencia.

- **Disponibilidad**: asegurar que la información esté accesible cuando se necesita, sin interrupciones indeseadas.

Estos tres pilares no operan de forma aislada: conforman un sistema simétrico donde un fallo en uno compromete todo el esquema. Una falla en confidencialidad puede dañar la reputación; en integridad, cuestionar la fiabilidad; y en disponibilidad, paralizar procesos críticos.

2. Evaluación de riesgos y controles eficaces

Un enfoque reactivo no basta. Es imprescindible adoptar una visión preventiva que incluya:

- **Evaluación de riesgos**: identificación de amenazas, vulnerabilidades y evaluación de impactos en la organización.

- **Políticas y controles**: definir reglas de acceso, cifrado, autenticación multifactor, segmentación de redes, y controles físicos y técnicos.

- **Formación y concienciación**: asegurar que el personal conozca su rol y las amenazas como phishing o uso de redes públicas.

Este enfoque sistemático permite **amplificar** la protección en lugar de limitarse a reaccionar cuando ya ha ocurrido un incidente (transformación natural del método PASTOR).

Ejemplos de gobernanza débil: beneficios y desventajas

La **gobernanza débil** en una organización no siempre se manifiesta de forma evidente. En muchos casos, se infiltra lentamente a través de decisiones erráticas, estructuras laxas, falta de control o conflictos de interés no gestionados. Si bien puede parecer que cierta flexibilidad favorece la innovación o agilidad, la experiencia demuestra que sus efectos, tarde o temprano, generan consecuencias costosas en términos de reputación, cumplimiento normativo y valor empresarial.

Este artículo analiza **ejemplos reales de gobernanza débil**, sus aparentes beneficios iniciales y las desventajas estructurales que pueden comprometer la viabilidad de una empresa. También se plantea cómo evitar estos errores mediante una gobernanza sólida.

¿Qué es la gobernanza débil?

La **gobernanza débil** se refiere a la ausencia o mal funcionamiento de los mecanismos que garantizan una gestión empresarial ética, eficiente y alineada con los intereses de todos los grupos de interés. Esto puede incluir:

01. **Falta de supervisión efectiva por parte del consejo de administración.**

02. **Procesos de toma de decisiones poco transparentes o concentrados en pocas personas.**

03. **Ausencia de controles internos sólidos o canales de denuncia.**

04. **Conflictos de interés sin gestionar.**

En estas condiciones, es común que se generen decisiones poco informadas, riesgos mal gestionados y comportamientos poco éticos. Lo preocupante es que, al principio, puede parecer que una menor burocracia facilita el crecimiento.

Ejemplos reales de gobernanza débil

El caso de la empresa **Clarivate**, analizado por Radical Compliance, es un ejemplo reciente y revelador. En 2023, su CEO aprobó una modificación sustancial de su propio contrato sin notificarlo debidamente al consejo. Cuando se descubrió, se corrigió, pero el daño reputacional ya estaba hecho. El error se originó en una **estructura poco clara** y una delegación de autoridad mal definida, donde no estaba claro quién debía aprobar ciertos cambios contractuales.

Otros casos históricos de gobernanza débil incluyen:

- **Enron**: donde la opacidad contable y la complacencia del consejo permitieron una crisis de magnitud global.

Nuevos avances en normativa sobre ciberseguridad

La **normativa sobre ciberseguridad** está viviendo una transformación acelerada en respuesta al crecimiento exponencial de los riesgos digitales. Las amenazas se han vuelto más sofisticadas, el impacto de los ciberataques es más severo que nunca y las expectativas regulatorias aumentan cada año. Para las organizaciones, adaptarse a este nuevo entorno ya no es una opción, sino una necesidad crítica.

En este artículo, exploramos los principales avances legislativos y tendencias en torno a la normativa sobre ciberseguridad a nivel global. Analizamos cómo las nuevas regulaciones impactan a las empresas y qué acciones pueden tomar para estar alineadas con los estándares actuales, evitando sanciones y fortaleciendo su resiliencia digital.

Un entorno regulatorio cada vez más exigente

En los últimos años, los reguladores han pasado de enfoques genéricos a **normativas específicas, detalladas y proactivas**.

Esta evolución busca garantizar que las organizaciones no solo respondan a los incidentes cibernéticos, sino que implementen medidas preventivas robustas.

En Estados Unidos, la **SEC (Securities and Exchange Commission)** introdujo en 2023 nuevas reglas de **divulgación obligatoria de incidentes cibernéticos**, exigiendo a las empresas que reporten cualquier incidente material dentro de un plazo máximo de cuatro días. Esta medida busca garantizar la transparencia y reducir la asimetría de información con los inversores.

En Europa, el reglamento **NIS2**, que entrará plenamente en vigor en 2025, amplía significativamente las obligaciones en materia de ciberseguridad. Esta directiva exige a entidades públicas y privadas adoptar planes de gestión de riesgos, realizar auditorías periódicas y contar con mecanismos de respuesta ante incidentes.

Tendencias globales: de la reacción a la prevención

Además del endurecimiento normativo, se observa una clara tendencia hacia una **gobernanza integral de la ciberseguridad**. Las organizaciones están llamadas a implementar marcos de gestión de riesgos digitales alineados con estándares como ISO/IEC 27001, NIST CSF o COBIT, que permitan integrar la ciberseguridad en la estrategia corporativa.

Estas nuevas normas promueven una **visión proactiva y basada en el riesgo**, que abarca desde la evaluación del contexto hasta la definición de roles y responsabilidades claras en materia de seguridad de la información.

GRI: Mejorando la Transparencia y la Confianza en el Reporting Corporativo

En un entorno empresarial cada vez más exigente, **la transparencia y la rendición de cuentas** se han convertido en pilares fundamentales para mantener la confianza de los grupos de interés. Los inversores, consumidores, empleados y reguladores ya no se conforman con promesas: exigen datos claros, verificables y comparables sobre el impacto social, ambiental y económico de las organizaciones. En este contexto, el estándar **GRI** (Global Reporting Initiative) ha emergido como una de las herramientas más eficaces para fortalecer el reporting corporativo y demostrar el compromiso con la sostenibilidad.

Este artículo explora qué es GRI, cómo mejora la credibilidad de las empresas y cuáles son sus beneficios estratégicos. Además, veremos cómo la tecnología puede ayudar a cumplir con sus exigencias de manera eficiente.

¿Qué es GRI y por qué es relevante?

GRI es una organización internacional independiente que proporciona un marco global para la **elaboración de informes de sostenibilidad**. Sus estándares permiten a las organizaciones informar públicamente sobre sus impactos en la economía, el medio ambiente y la sociedad, de forma sistemática y estandarizada.

Lo que distingue a los estándares GRI es su enfoque centrado en las **expectativas de las partes interesadas**. En lugar de priorizar únicamente la rentabilidad o los objetivos internos, GRI obliga a mirar hacia afuera: ¿qué preocupa a los grupos de interés? ¿Qué impactos debe gestionar y reportar la empresa para ser considerada responsable?

Adoptar el marco GRI no solo mejora la calidad del reporting, sino que fortalece la legitimidad de la organización y genera valor a largo plazo.

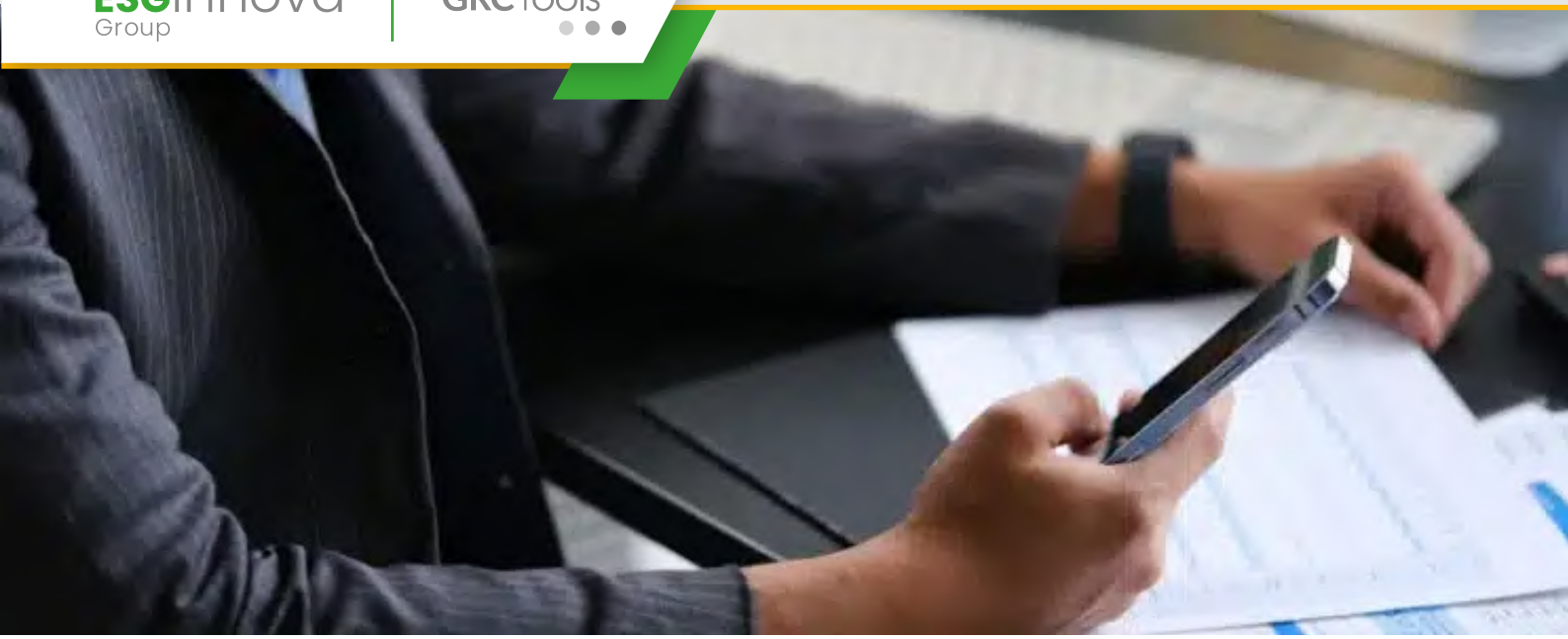
Beneficios clave de aplicar GRI en las organizaciones

Implementar los estándares GRI ofrece **múltiples ventajas estratégicas**, entre las que destacan:

- **Mayor transparencia y confianza**: Al divulgar de manera estructurada los impactos económicos, ambientales y sociales, las organizaciones construyen relaciones de confianza con sus stakeholders.

- **Mejor toma de decisiones**: El proceso de recopilación, análisis y presentación de datos facilita el conocimiento profundo del desempeño no financiero de la empresa.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo dar cumplimiento a la Ley Karin 21643 con un canal de denuncias

La reciente entrada en vigor de la **Ley Karin 21.643** en Chile ha supuesto un punto de inflexión en la forma en que las organizaciones abordan el acoso laboral, sexual y la violencia en el trabajo. Esta normativa, cuyo objetivo es **prevenir y sancionar conductas indebidas en el entorno laboral**, obliga a empleadores públicos y privados a establecer mecanismos eficaces para la recepción, gestión y resolución de denuncias. En este nuevo contexto, **el canal de denuncias** se consolida como una herramienta indispensable para el cumplimiento legal y la protección de las personas trabajadoras.

Este artículo explora qué exige la Ley Karin, cómo se articula el canal de denuncias como pieza clave del sistema de cumplimiento, y cuáles son las ventajas estratégicas que aporta su correcta implementación.

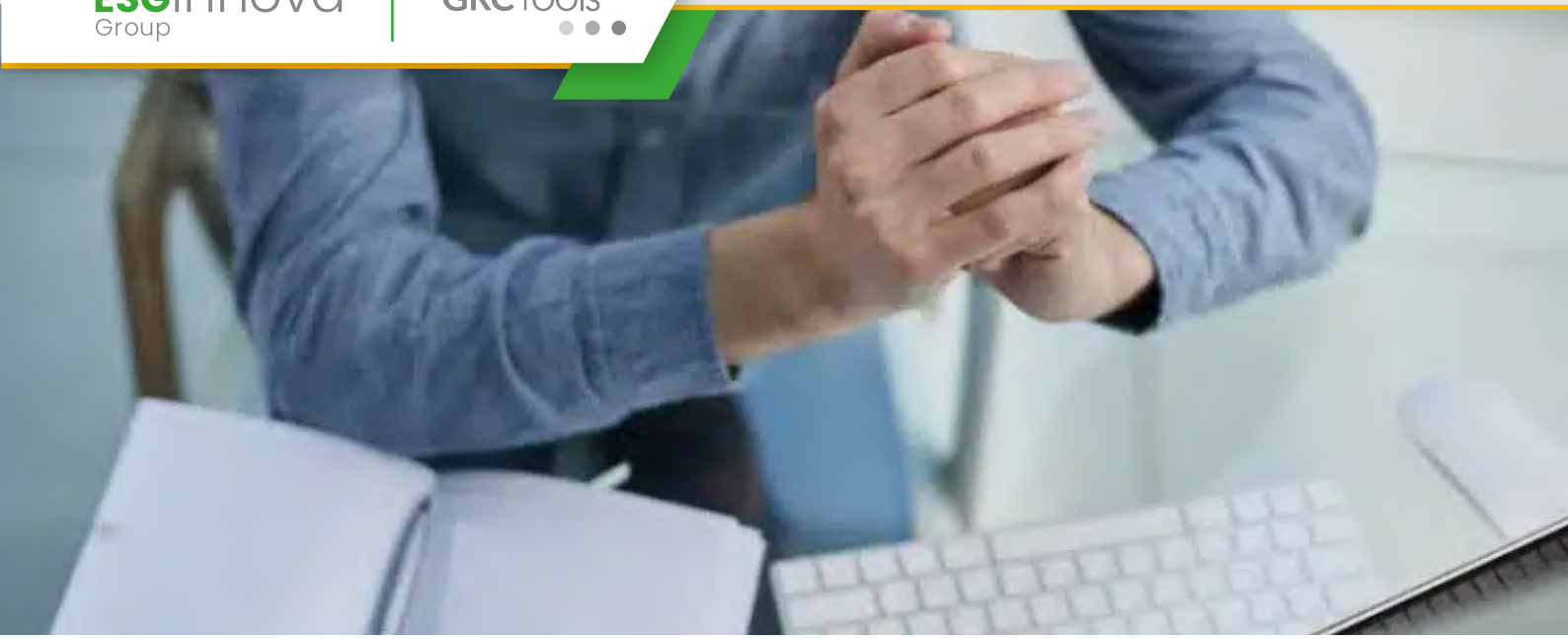
¿Qué establece la Ley Karin 21.643?

Promulgada en enero de 2024, la Ley Karin modifica el Código del Trabajo y otras normativas relacionadas, con el fin de **prevenir y sancionar el acoso laboral, el acoso sexual y la violencia en el trabajo**, fortaleciendo los protocolos existentes y estableciendo nuevos deberes para los empleadores. Algunos de los elementos más relevantes son:

- **Obligación de contar con un canal de denuncias confidencial y seguro** para que las víctimas o testigos puedan reportar hechos sin temor a represalias.
- **Protocolos claros y formales** para la recepción, tramitación, investigación y resolución de los casos denunciados.
- **Medidas de protección a las víctimas y denunciantes**, incluyendo la confidencialidad, el resguardo de la integridad psicológica y física, y la no discriminación.
- **Capacitación periódica** a trabajadores y empleadores en temas de prevención, detección temprana y abordaje de estos hechos.
- **Registro y trazabilidad** de todos los procesos relacionados con la denuncia.

En síntesis, la ley exige no solo reaccionar ante hechos de acoso, sino prevenir activamente su ocurrencia y garantizar un entorno laboral libre de violencia.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo se puede aplicar la gestion de riesgos a tu proyecto empresarial

Emprender un proyecto empresarial implica una combinación de visión, estrategia y acción, pero también una correcta identificación de amenazas y vulnerabilidades que podrían comprometer el éxito. Es aquí donde entra en juego la **gestión de riesgos**, una disciplina esencial para anticipar lo inesperado, minimizar impactos negativos y maximizar las oportunidades.

Lejos de ser una tarea exclusiva de grandes corporaciones, **la gestión de riesgos es vital desde la etapa inicial de cualquier emprendimiento**. Ya sea que estés lanzando una startup tecnológica, un nuevo servicio o expandiendo tu empresa, implementar un enfoque estructurado ante los riesgos marcará la diferencia entre la resiliencia y el fracaso.

¿Qué es la gestión de riesgos?

La **gestión de riesgos** es el conjunto de procesos que permite identificar, evaluar y controlar los riesgos que pueden afectar el logro de los objetivos empresariales. Se basa en un enfoque sistemático que contempla tanto factores internos como externos que podrían derivar en pérdidas financieras, interrupciones operativas, problemas legales, daños reputacionales, entre otros.

Un sistema de gestión de riesgos bien aplicado te permite:

- **Detectar amenazas potenciales** antes de que se materialicen.
- **Evaluar su impacto y probabilidad**, priorizando aquellos con mayor gravedad.
- **Definir planes de respuesta**, desde la prevención hasta la mitigación o aceptación.
- **Monitorear continuamente el entorno** para adaptar la estrategia ante nuevas condiciones.

Es, en resumen, un ejercicio de previsión, protección y mejora continua.

¿Por qué integrar la gestión de riesgos en tu proyecto?

Muchos proyectos empresariales fracasan no por falta de talento o creatividad, sino por no anticipar los obstáculos. Invertir tiempo en la **gestión de riesgos** al inicio del proyecto permite establecer bases sólidas que favorezcan la toma de decisiones con mayor información y menor incertidumbre.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué son los requisitos temáticos de ciberseguridad?

En un entorno cada vez más digitalizado, la ciberseguridad ha dejado de ser un asunto exclusivamente técnico para convertirse en una cuestión estratégica y transversal. Las amenazas informáticas evolucionan con rapidez, afectando no solo a la infraestructura tecnológica, sino también a la reputación, cumplimiento normativo y sostenibilidad de las organizaciones. En este contexto, surgen los **requisitos temáticos de ciberseguridad**, una propuesta que busca estructurar y estandarizar las expectativas sobre cómo las entidades deben gestionar su protección digital.

Estos requisitos se están posicionando como una referencia para auditores, profesionales del **compliance** y responsables de gobernanza, ya que ofrecen un marco más claro y coherente para evaluar y fortalecer los controles de ciberseguridad. Pero ¿en qué consisten realmente y por qué su implementación se ha vuelto prioritaria?

¿Qué son los requisitos temáticos de ciberseguridad?

Los **requisitos temáticos de ciberseguridad** son criterios organizados en torno a temas clave que abordan diferentes dimensiones de la protección digital. A diferencia de marcos puramente técnicos o normativos, estos requisitos adoptan una visión integral y práctica, enfocada en los riesgos reales a los que se enfrentan las organizaciones.

Entre los principales temas abordados se incluyen:

- **Gobierno de la ciberseguridad**: establecimiento de roles, políticas, recursos y liderazgo.
- **Evaluación de riesgos digitales**: identificación, análisis y tratamiento de amenazas tecnológicas.
- **Controles de protección**: medidas técnicas y organizativas para prevenir accesos no autorizados.
- **Respuesta ante incidentes**: preparación, detección, contención y recuperación frente a ataques.
- **Concienciación y formación**: capacitación del personal para reducir el riesgo humano.
- **Supervisión y mejora continua**: seguimiento de controles, auditorías y ajustes proactivos.

Cada tema funciona como un pilar desde el cual se pueden desarrollar políticas robustas, estrategias de prevención y planes de acción en caso de emergencia.

¿Qué es la carta de auditoría interna?

En el ecosistema del **Gobierno Corporativo**, la **auditoría interna** se ha consolidado como una función esencial para garantizar la integridad, la eficiencia y el cumplimiento dentro de las organizaciones. Sin embargo, existe un documento clave que muchas veces pasa desapercibido incluso por los propios comités de auditoría: la **Carta de Auditoría Interna**.

Este documento, que debería ser el **marco fundacional** de la actividad de auditoría interna, es más que una simple formalidad. Define **autoridad, responsabilidad, alcance e independencia**, y establece la relación que la función de auditoría interna tiene con el consejo de administración, el comité de auditoría, la alta dirección y otras áreas.

¿Qué es exactamente la Carta de Auditoría Interna?

La **Carta de Auditoría Interna** es un documento formal, aprobado por el **consejo de administración o el comité de auditoría**, que autoriza la existencia de la función de auditoría interna, y define

su **misión, propósito, independencia, responsabilidades y autoridad** dentro de la organización.

Según los **Estándares Internacionales para el Ejercicio Profesional de la Auditoría Interna (GIAS, por sus siglas en inglés)**, este documento es **obligatorio**. No solo es un requisito técnico, sino también una herramienta estratégica para reforzar la legitimidad de la función de auditoría.

¿Por qué es tan importante?

Aunque pueda parecer un simple documento administrativo, la **Carta de Auditoría Interna** cumple múltiples funciones críticas:

- **Otorga legitimidad e independencia**: al estar aprobada por el consejo o comité de auditoría, garantiza que la auditoría interna tenga la **autoridad necesaria** para operar de forma objetiva.
- **Define el alcance del trabajo**: delimita las áreas sobre las que la auditoría puede actuar, incluyendo procesos, sistemas, filiales, riesgos, etc.
- **Establece la relación jerárquica y funcional**: aclara a quién reporta el auditor interno, generalmente al comité de auditoría en el plano funcional y al CEO en el plano administrativo.
- **Fortalece el cumplimiento de normas internacionales**: tanto los GIAS como el Marco Internacional para la Práctica Profesional de la Auditoría Interna (IPPF) recomiendan su revisión **al menos una vez al año**.

La importancia del analista de cumplimiento para apoyar la gestión de riesgos

Con un marco regulatorio en constante transformación y con estándares de cumplimiento cada vez más exigentes, el papel del **analista de cumplimiento** ha pasado de ser secundario a convertirse en un elemento central de las estrategias corporativas para gestionar riesgos y garantizar la integridad organizacional. Este profesional, además de velar por el cumplimiento normativo, también se ha convertido en una figura clave en la **gestión de riesgos empresariales**, alineando los objetivos legales, éticos y estratégicos de la empresa.

Contar con un analista de cumplimiento sólido y proactivo no es una opción, sino una inversión esencial. Las organizaciones que ignoran esta figura o la subestiman se exponen a sanciones, pérdidas económicas y deterioro reputacional. Por el contrario, aquellas que entienden su valor incorporan al cumplimiento como parte fundamental de su **modelo de prevención** y control de riesgos.

Cumplimiento y gestión de riesgos: una relación estratégica

El analista de cumplimiento desempeña un papel decisivo al identificar, evaluar y mitigar riesgos relacionados con normativas legales, códigos de conducta y políticas internas. Su función va más allá del control formal: implica **anticipar escenarios**, comprender el **contexto operativo** y proponer **acciones correctivas o preventivas** con base en datos verificables.

Además, trabaja en colaboración con distintas áreas de la organización —legal, auditoría, calidad, recursos humanos— para garantizar que el cumplimiento no sea un esfuerzo aislado, sino una **práctica transversal integrada** en todos los procesos clave.

Gracias a esta visión global, el analista contribuye directamente a la consolidación de una **cultura de integridad**, mejora la toma de decisiones y refuerza la transparencia ante los grupos de interés.

Un perfil profesional en evolución

Tradicionalmente vinculado al ámbito jurídico, el **analista de cumplimiento** moderno necesita competencias multidisciplinarias. Además del conocimiento normativo, debe manejar herramientas de gestión de riesgos, dominar metodologías de **auditoría interna**, utilizar indicadores clave de desempeño (**KPI**) y ser capaz de comunicar con claridad.

Se espera que supervise **novedades legislativas y proponga actualizaciones de políticas y procedimientos** cuando sea necesario.

¿Cómo abordar la complejidad de la CSRD de la Unión Europea?

La **CSRD de la Unión Europea** (Corporate Sustainability Reporting Directive) ha marcado un antes y un después en la forma en que las organizaciones deben reportar su desempeño en **sostenibilidad**. Más que un requisito legal, representa un cambio de paradigma: pasar de informes voluntarios y, en muchos casos, superficiales, a reportes exhaustivos, auditables y alineados con estándares internacionales como los del **EFRAG** o el **Global Reporting Initiative (GRI)**.

Para las empresas que operan en la UE —o que forman parte de cadenas de suministro vinculadas a este mercado— el desafío no es solo cumplir, también tienen que integrar la CSRD en su estrategia corporativa. Esto implica desarrollar procesos robustos de recopilación y gestión de datos, establecer indicadores clave (KPIs) medibles y garantizar la transparencia ante inversores, clientes, autoridades y demás grupos de interés.

El impacto estratégico de la CSRD

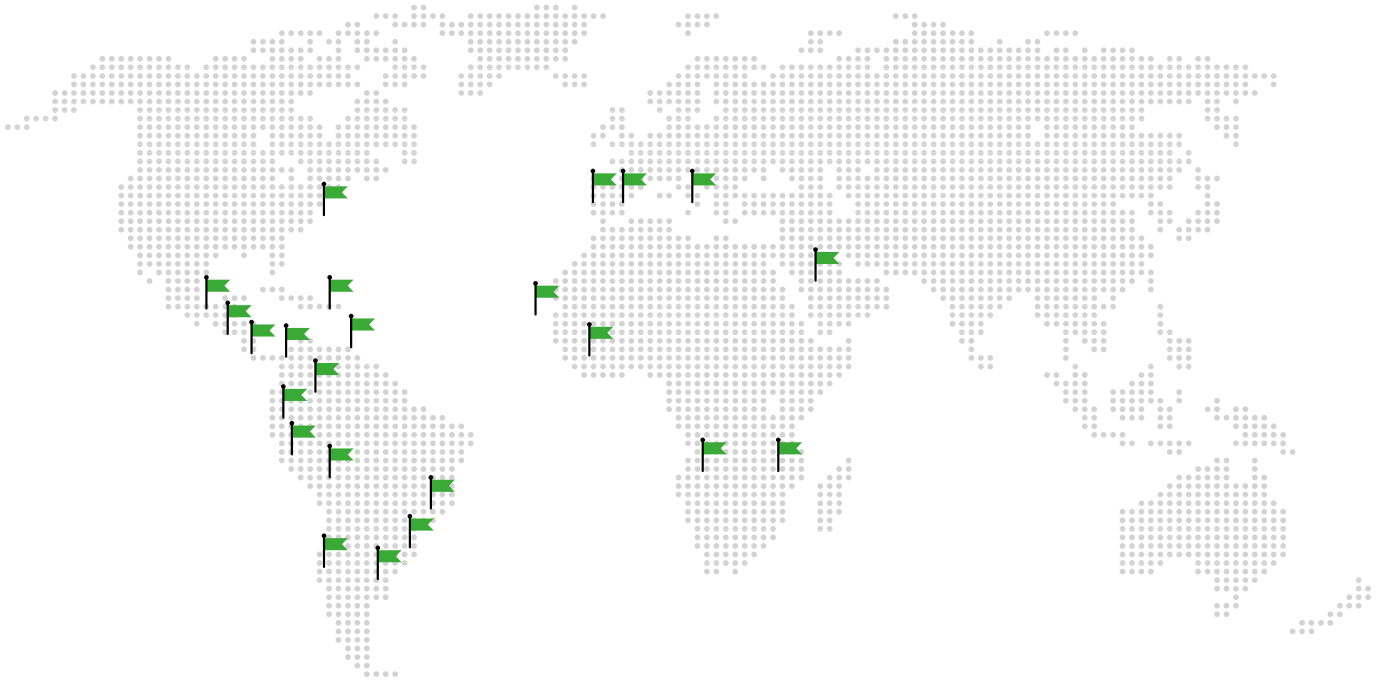
La **CSRD de la Unión Europea** amplía de manera significativa el alcance de la antigua **Directiva de Información No Financiera** (NFRD). Ahora incluye a muchas más empresas, independientemente de su sector, y exige información detallada sobre aspectos ambientales, sociales y de gobernanza (ESG). Esto significa que organizaciones que antes no estaban obligadas a reportar ahora deben prepararse para cumplir con un marco normativo exigente, que abarca desde la huella de carbono y el uso de recursos hasta políticas de diversidad, igualdad salarial y derechos humanos en la cadena de suministro.

Además, la directiva exige que la información esté **verificada por terceros**, lo que incrementa la necesidad de contar con datos precisos, trazables y respaldados por evidencias documentales. Esto eleva el cumplimiento a un nuevo nivel, donde la improvisación no tiene cabida y la tecnología se convierte en una aliada imprescindible.

Retos clave para las organizaciones

Abordar la **CSRD de la Unión Europea** implica gestionar un alto volumen de información proveniente de múltiples departamentos, filiales y socios estratégicos. Entre los retos más comunes destacan:

- Consolidar datos ESG dispersos en diferentes formatos y sistemas.
- Alinear las métricas internas con los **Estándares Europeos de Información sobre Sostenibilidad (ESRS)**.
- Establecer controles internos que aseguren la calidad y consistencia de la información.



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