EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

MARZO 2025

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.

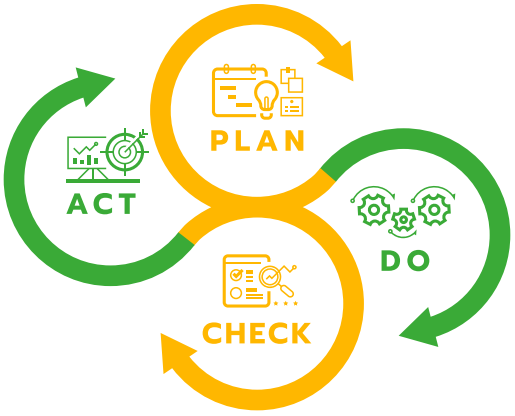
Plataforma ESG Innova

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

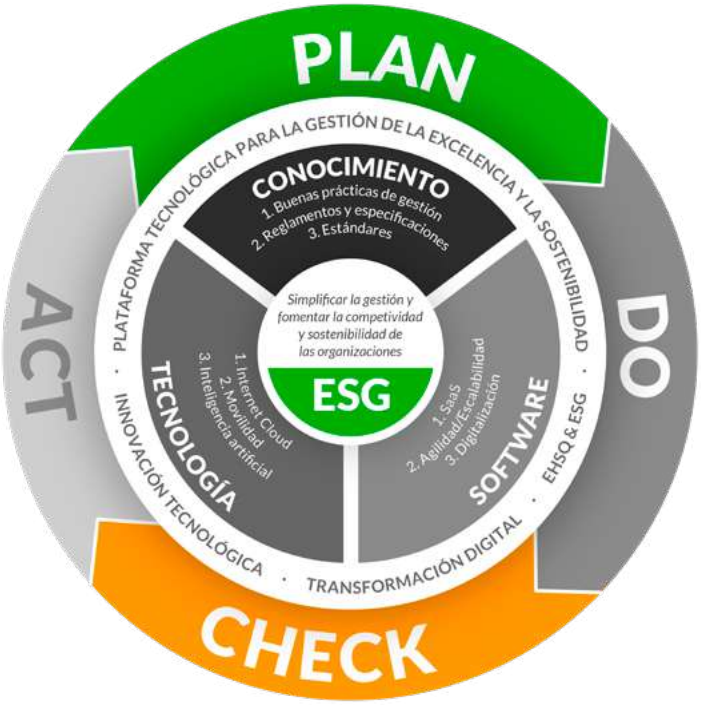
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ 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

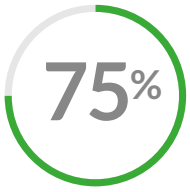
Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento.

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

Menos de tiempo de resolución de una acción correctiva

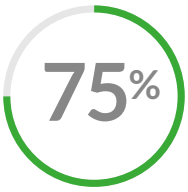
Menos de tiempo de preparación de las reuniones de gestión



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**

ISOTools, líder en automatizar ISO 9001 e ISO 42001, en el Foro de la Calidad 2025

El **Foro Internacional de la Calidad**, organizado por **ICONTEC** en Cartagena de Indias (**Colombia**) durante **agosto de 2025**, es mucho más que un evento: es un punto de encuentro para los líderes, expertos y profesionales que están definiendo el futuro de la gestión de la calidad en Latinoamérica y el mundo. Desde su primera edición, este foro ha sido un referente para compartir conocimientos, tendencias y buenas prácticas en un entorno donde la innovación y la transformación digital son claves para el éxito empresarial. En su edición 2025, el foro promete superar todas las expectativas, consolidándose como el espacio ideal para explorar cómo las organizaciones pueden adaptarse a los nuevos desafíos y oportunidades que presenta la era de la **Calidad 4.0**.

En este contexto, **ISOTools**, la plataforma tecnológica líder en la automatización de sistemas de gestión basados en normas ISO, se prepara para participar activamente en este prestigioso evento. Nuestra presencia en el Foro de la Calidad 2025 busca reforzar

el compromiso con la excelencia y la innovación, a la vez que nos permite demostrar cómo nuestras soluciones están ayudando a las empresas a implementar y mantener normas como la **ISO 9001** y la **ISO 42001** de manera eficiente y efectiva.

El Foro de la Calidad 2025: Un evento que marca tendencias

El **Foro Internacional de la Calidad** es, sin duda, el evento más importante en su categoría en Latinoamérica. Con más de 15 ediciones, ha logrado consolidarse como un espacio donde se discuten y se anticipan las tendencias que están transformando la gestión de la calidad a nivel global. La edición 2025 no será la excepción, ya que abordará temas críticos para el futuro de las organizaciones, como:

- **Calidad 4.0**: Cómo las tecnologías emergentes, como la inteligencia artificial (IA), el Internet de las cosas (IoT) y el big data, están redefiniendo los sistemas de gestión.

- **Transformación digital**: Estrategias para integrar la digitalización en los procesos empresariales y mejorar la eficiencia operativa.

- **Actualizaciones normativas**: Los últimos cambios en normas internacionales como la **ISO 9001**, **ISO 14001**, **ISO 45001** y, especialmente, la **ISO 42001**, que establece los lineamientos para la gestión de sistemas de inteligencia artificial.

Además, el foro contará con la participación de expertos internacionales, líderes empresariales y representantes de organizaciones exitosas que compartirán sus experiencias y aprendizajes. Esto lo convierte en una oportunidad única para **aprender**, **conectar** e **inspirarse**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Implementación de DORA: paso a paso para cumplir con la regulación sobre la resiliencia operativa digital

Empresas financieras, grandes y pequeñas, así como organizaciones de TI que provean productos o servicios a las primeras avanzan en la **implementación de DORA**. Los requisitos de la regulación sobre resiliencia operativa digital son complejos y el cumplimiento requiere definir gobernanza, implementar medidas de **seguridad de la información** y de ciberseguridad y gestionar los riesgos de continuidad del negocio, entre otras de igual relevancia.

Es importante aclarar que la implementación de DORA **es un tanto más simple para empresas pequeñas del sector financiero**. Estas organizaciones hacen uso de un marco simplificado para gestionar los riesgos. La siguiente guía pretende ser un instrumento de utilidad tanto para organizaciones grandes o proveedoras de TI como para aquellas otras de menor envergadura.

Cuáles son los pasos para realizar la implementación de DORA

La implementación de DORA **guarda algunas similitudes con la implementación de un sistema de gestión**. Por eso, y por la coincidencia en muchos de los objetivos, las organizaciones que han implementado **ISO 27001**, estándar de seguridad de la información, encontrarán la tarea mucho más fácil. En ella es necesario avanzar por una serie de fases.

1. Realizar un análisis de brechas

Algunas de las solicitudes de DORA pueden ya estar resueltas en la organización, sobre todo si, como ya se advierte, ha implementado ISO 27001. El objetivo del análisis GAP, o análisis de brechas, es **establecer qué hay, qué es útil y qué falta para llegar a la conformidad total.**

2. Obtener el aval de la Alta Dirección

Aunque la implementación de DORA no es opcional para las empresas que deben **cumplir con el Reglamento de Resiliencia Operativa Digital**, es importante que la Alta Dirección conozca y apruebe el proyecto por dos razones: **será este el órgano encargado de asignar los recursos** y es también el único autorizado para tomar decisiones sobre temas críticos como privacidad de datos o seguridad de la información.

3. Planificar la implementación de DORA

Como todo proyecto estratégico, **la organización necesita tener un plan minucioso.**

Documentación ISO 42001 esencial para el cumplimiento y la certificación del estándar de IA

La **documentación ISO 42001** es uno de los aspectos más importantes en la implementación de un sistema de gestión de IA. Alcanzar el cumplimiento con todos los requisitos de la norma implica generar todos los documentos solicitados por esta, verificando la acertada comunicación con las partes interesadas, la accesibilidad a las personas indicadas, la trazabilidad en las actualizaciones y la garantía de confidencialidad e integridad de la información.

La documentación ISO 42001 obligatoria **se agrupa en once categorías**. En algunas se habla de un solo documento, mientras que en otras se hace referencia a un grupo de documentos o a todos los que se produzcan con el mismo propósito. La política, por ejemplo, es solo una. Los acuerdos con terceros, en cambio, serán tantos como los suscriba la organización.

Documentación ISO 42001 obligatoria

1. Política de gestión de sistemas de IA y de seguridad de la información

Pueden ser dos documentos o uno solo que reúna el **compromiso de la Alta Dirección con el desarrollo o uso responsable de sistemas de IA** y, a la vez, con la privacidad de los datos y la seguridad de la información. Las organizaciones que han implementado ISO 27001 no necesitarán producir **políticas de seguridad de la información**.

El documento también **fija los objetivos generales** y expresa la decisión de asignar y entregar los recursos necesarios. Este es el documento que le imprime el tono superior al proyecto, necesario en todas las instancias de implementación, certificación y mantenimiento.

2. Evaluaciones de riesgos

Es un ejemplo de documentación ISO 42001 que se produce con la operación rutinaria del sistema de gestión de riesgos de la IA. Todas las **evaluaciones de riesgos se documentan** y en ellas se detallan los riesgos identificados y las acciones de gestión propuestas, así como las metodologías que se utilizaron.

3. Evaluaciones de impacto sobre la protección de datos

Las evaluaciones de impacto sobre protección de datos **son obligatorias para las empresas que tratan con grandes volúmenes de información confidencial**.

Publicada la nueva ISO 37001:2025

La lucha contra el soborno y la corrupción es una prioridad global para las organizaciones que buscan operar con integridad y transparencia. En este contexto, la publicación de la **nueva ISO 37001:2025** marca un **momento clave** en la evolución de los Sistemas de Gestión Antisoborno (SGAS). Esta segunda edición, desarrollada por el **Comité Técnico ISO/TC 309** sobre Gobernanza de las organizaciones, reemplaza a la versión anterior (ISO 37001:2016) e incorpora importantes actualizaciones técnicas y conceptuales.

A continuación, exploraremos las **principales actualizaciones de la norma**, su **importancia para el sector empresarial** y cómo el **Software ISO 37001 de ISOTools** se convierte en un aliado estratégico para su implementación eficiente y efectiva.

¿Qué es ISO y cómo se desarrolla la norma ISO 37001?

La **Organización Internacional de Normalización (ISO)** es una federación mundial de organismos nacionales de normalización. Su trabajo se realiza a través de **comités técnicos**, donde cada miembro

interesado en un tema tiene derecho a estar representado. En el caso de la ISO 37001, el **Comité Técnico ISO/TC 309** fue responsable de su desarrollo, contando con la participación de organizaciones internacionales, gubernamentales y no gubernamentales.

Este documento fue redactado siguiendo las **Directivas ISO/IEC, Parte 2**, que establecen las reglas editoriales y los procedimientos para la elaboración y mantenimiento de las normas. Además, ISO colabora estrechamente con la **Comisión Electrotécnica Internacional (IEC)** en temas de normalización, asegurando coherencia y calidad en sus publicaciones.

Es importante destacar que las normas ISO son de **aplicación voluntaria** y no constituyen una obligación legal. Sin embargo, su adopción es una herramienta poderosa para alinear las prácticas organizacionales con los principios de la **Organización Mundial del Comercio (OMC)** y superar los **Obstáculos Técnicos al Comercio (OTC)**.

¿Qué cambia en la ISO 37001:2025?

La **ISO 37001:2025** llega con actualizaciones significativas que reflejan las lecciones aprendidas desde su primera edición (2016) y responden a los nuevos retos en la gestión del soborno. Algunos de los cambios más destacados incluyen:

01. Enfoque en el cambio climático y la cultura de cumplimiento:

- Se añadieron subcláusulas que vinculan la gestión antisoborno con la sostenibilidad y la responsabilidad ambiental, reconociendo el impacto del **cambio climático** en los riesgos de corrupción.

Análisis de causa raíz: 3 herramientas clave para realizarlo con éxito

Dentro de los sistemas de gestión de calidad basados en **ISO 9001**, el **análisis de causa raíz** es una de las herramientas más útiles para solucionar problemas, eliminar la posibilidad de repetición, optimizar procesos, promover una mejora continua real y evidente e identificar riesgos ocultos que no han sido tratados por los expertos en gestión de riesgos.

El manual de procedimiento indica que hay que resolver los problemas y las **no conformidades de calidad**, **diseñando e implementando acciones correctivas eficaces**. El desafío está en que algunos fallos de calidad sugieren una solución primaria que apunta a resolver la manifestación evidente e inmediata del problema, que es la que sale a la superficie. Es una solución que no ahonda en su origen real, persistiendo la probabilidad de repetición, salvo que se realice un análisis de causa raíz.

Cómo realizar un análisis de causa raíz

El objetivo del análisis de causa raíz es llegar el origen de un problema. Por supuesto, problemas complejos demandarán investigaciones igualmente complejas. En términos generales, sin tener en cuenta aún la herramienta seleccionada para practicar el análisis de causa raíz, hay unos pasos que es importante seguir:

- **Identificar y documentar el problema con precisión**: lugar en el que se hizo evidente el problema, señales exhibidas, producto o línea de productos afectados, procesos asociados, consecuencias y gravedad.

- **Determinar el alcance del impacto negativo** en caso de que el problema no se investigue y se trate con la debida celeridad.

- **Señalar factores o condiciones** que pueden estar asociados a la generación del problema.

- **Asignar la investigación** a un profesional experto o a un equipo dedicado capacitado para realizar el análisis de causa raíz.

- **Elegir una metodología** o herramienta adecuada para realizar el análisis.

La complejidad y el tamaño de la organización, y en consecuencia de los problemas, determinará la necesidad de conformar un equipo o asignar la tarea a una sola persona. **El análisis de causa raíz es un tipo de evaluación básico**. Pese a ello, en algunos casos puede involucrar aspectos técnicos e incluso científicos tan complejos, que puede ser necesario la participación de expertos de diferentes áreas de la organización.

Roles y responsabilidades en ISO 42001: claves para la gestión y desarrollo de sistemas de IA

Asignar **roles y responsabilidades en ISO 42001** es uno de los pasos que conforman el proceso de implementación de un sistema de gestión de Inteligencia Artificial basado en el estándar de ISO. Es, además, una de las formas en las que la alta dirección demuestra liderazgo.

Una vez el SGIA se ha implementado y certificado, **se mantienen las asignaciones pensando en el mantenimiento y mejora continua del sistema**. Por eso es tan importante saber qué personas asumirán los roles y responsabilidades en ISO 42001. También es necesario saber dónde encontrarlas y definir un perfil adecuado para ellas en el que se consideren criterios como conocimiento, experiencia y competencias.

Cuál es la importancia de ISO 42001

ISO 42001 es el **primer estándar de sistemas de gestión IA** de alcance internacional.

La norma, que puede ser utilizada por todo tipo de organizaciones de cualquier tamaño, complejidad y procedencia, **entrega requisitos, orientaciones y controles para tratar los riesgos asociados al uso de la Inteligencia Artificial**, entre ellos privacidad de datos, toma de decisiones con base en información sesgada, cumplimiento legal, derechos humanos y transparencia.

El uso de Inteligencia Artificial plantea reticencias en las personas y estas crean incertidumbre en el ámbito corporativo. Es lo que motivó la publicación de un estándar eficaz para gestionar los riesgos y **garantizar el uso responsable, ético, transparente y legal de la nueva tecnología**.

Se trata de una **tecnología que está en constante evolución**, lo que representa un desafío para el aún nuevo estándar. Pero también es una razón para tomarse muy en serio la definición de roles y responsabilidades en ISO 42001 y la elección de las personas que asumirán esos puestos.

La estructura del estándar es un buen punto de partida para identificar los roles y responsabilidades en ISO 42001.

Es el siguiente paso **antes de elegir a las personas que tendrán a su cargo la operación del sistema de gestión de Inteligencia Artificial**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cambios más importantes de la nueva ISO 37001:2025

Principios fundamentales, como la **ética** y la **responsabilidad**, guían a las organizaciones hacia un desempeño sostenible y confiable. En este escenario, combatir el soborno y la corrupción se ha convertido en una prioridad estratégica para empresas que buscan fortalecer su reputación y cumplir con los más altos estándares de conducta. La publicación de la nueva **ISO 37001:2025** representa un paso adelante en la evolución de los **Sistemas de Gestión Antisoborno (SGAS)**, ofreciendo un marco renovado y adaptado a los desafíos actuales.

Elaborada por el **Comité Técnico ISO/TC 309**, esta nueva edición sustituye a la versión anterior (ISO 37001:2016) e introduce actualizaciones técnicas y conceptuales significativas. Estos cambios reflejan las mejores prácticas aprendidas en los últimos años y responden a las exigencias de un entorno empresarial en constante transformación, desde la gestión de riesgos hasta la adopción de tecnologías emergentes.

¿Qué es la ISO 37001 y por qué es importante?

La **ISO 37001** es una norma internacional que establece los requisitos para implementar un **Sistema de Gestión Antisoborno (SGAS)**. Su objetivo es ayudar a las organizaciones a prevenir, detectar y gestionar el soborno, promoviendo una cultura de integridad y cumplimiento. Desde su primera edición en 2016, esta norma ha sido adoptada por empresas de todo el mundo como una herramienta clave para mitigar riesgos legales, reputacionales y financieros asociados al soborno.

La nueva versión, **ISO 37001:2025**, llega con actualizaciones significativas que reflejan las lecciones aprendidas en los últimos años y responden a los nuevos retos en la gestión del soborno. Estas mejoras refuerzan los principios de la norma, y también la alinean con las tendencias globales en sostenibilidad, tecnología y cumplimiento normativo.

Cambios clave de la ISO 37001:2025

1. Enfoque en el cambio climático y la sostenibilidad

Uno de los cambios más destacados de la nueva versión es la incorporación de subcláusulas que vinculan la gestión antisoborno con la **sostenibilidad** y la **responsabilidad ambiental**.

Este enfoque reconoce el impacto del cambio climático en los riesgos de corrupción, especialmente en sectores como la energía, la construcción y la minería. Las organizaciones deberán ahora considerar cómo sus prácticas antisoborno contribuyen a los **Objetivos de Desarrollo Sostenible (ODS)** de la ONU.

¿Qué hace que un sistema de control de documentos sea eficaz?

La gestión y el **control de documentos** son elementos esenciales para la seguridad y privacidad de la información. Las organizaciones dependen de sistemas de control de documentos confiables, seguros y eficientes, también aquellas que cuentan con **sistemas de gestión de Inteligencia Artificial**.

El control de documentos **garantiza disponibilidad, accesibilidad, trazabilidad, seguridad e integridad** de los documentos y, por extensión, de la información que contienen. Cuando todos estos elementos están presentes, no se pierde tiempo, no se generan conflictos, la productividad crece y el entorno de trabajo es cordial. Por supuesto, el cumplimiento es un agregado que no es desestimable.

Qué debe tener un sistema de gestión y control de documentos para ser eficaz

El control de documentos implica **asegurar una ubicación en la que las personas indicadas puedan acceder**, si su perfil de seguridad lo permite, a la información que requieran. El control de documentos también se ocupa de verificar que la versión a la que accedan sea la actual.

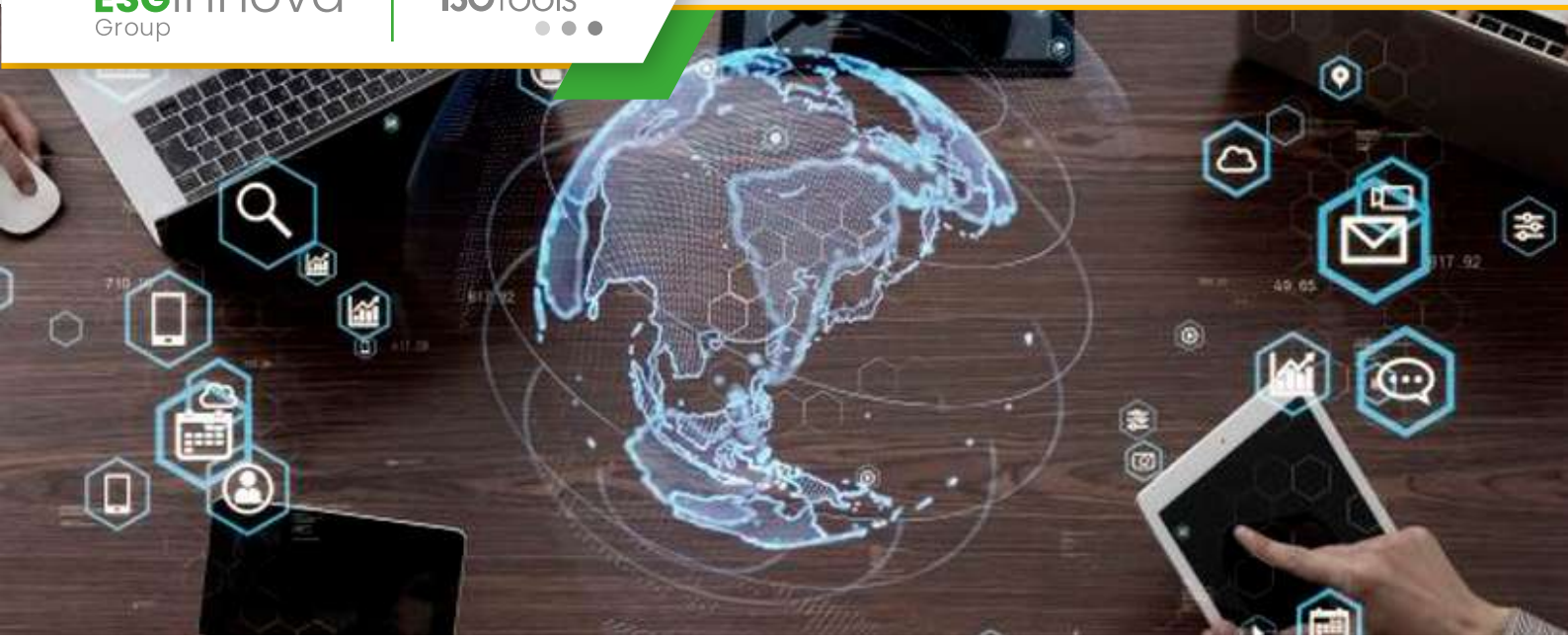
Además, entran en su ámbito de acción los procedimientos y protocolos necesarios para actualizar o revisar un documento.

De manera genérica, existen **ocho funcionalidades que no pueden faltar** en una solución o en un sistema para el control de documentos eficaz:

1. Protocolos y procedimientos para documentos específicos

Los documentos que se producen en una organización se podrían clasificar en grupos muy diferentes: manuales de procedimiento, legales, contratos, políticas o instrucciones de trabajo, por mencionar algunos entre los más recurrentes. Aun dentro del mismo grupo, un documento es diferente a otro.

El sistema de control de documentos necesita prever estas diferencias y **configurar flujos de creación y revisión acordes con el tipo de documento**, pero también crear protocolos de **seguridad de la información** y accesibilidad coherentes con la importancia y la confidencialidad del documento.



Soberanía de datos: concepto, retos y buenas prácticas

La **soberanía de datos** es un concepto que resulta de un punto de unión que encuentran las legislaciones y la tecnología. Leyes como el Reglamento General de Protección de Datos (RGPD) de la UE y otras regulaciones buscan preservar la privacidad de los datos y la seguridad de la información. Aspecto que también abordan estándares como **ISO 42001** en el marco de las organizaciones.

La soberanía de datos **ofrece un nuevo enfoque que responde a la creciente preocupación de los estados**. Esa preocupación está asociada a la vulnerabilidad que puede adquirir la información a causa de una falta de control sobre los datos que son procesados en los diferentes países.

Qué es la soberanía de datos

La soberanía de datos es el **derecho que reclaman los estados para controlar, gobernar y gestionar los datos que se generan dentro de los límites que marcan sus fronteras.**

Se incluyen los procesos y los instrumentos que se utilizan para recopilar, procesar, almacenar y transmitir esos datos.

Sobre el papel, la soberanía de datos está justificada por una ley, resultado de una demostración de gobernanza, que trata de ejercer un control tecnológico. La puesta en práctica no es tan fácil. **El primer desafío lo plantea es la inmensa, y aparentemente incontrolable, diversidad de fuentes de datos**: tiendas virtuales, asistentes controlados por IA, redes sociales, aplicaciones en dispositivos móviles, etc. A esta realidad se suma un agravante: **algunos de esos datos pueden implicar compromiso para la seguridad de las naciones** o estar asociados a actividades delictivas. Una de las formas en las que los estados ejercen la soberanía de los datos es promulgando normas como RGPD o la **Ley de Ciberresiliencia de la UE**.

Si bien la soberanía de datos representa un gran avance en el propósito de **garantizar la seguridad, confidencialidad e integridad de la información privada**, ha generado algunos conflictos entre países, atribuidos a vacíos en las respectivas legislaciones.

Existen datos que se comparten entre naciones, en virtud de acuerdos de cooperación comercial o judicial. En ese escenario, algunas naciones exigen que el procesamiento y almacenamiento se restrinja a sus fronteras, exigencia que no es siempre bien recibida en otras latitudes.

Por qué es importante la soberanía de datos

La soberanía de datos es fundamental porque **representa la autonomía de los gobiernos sobre su información y la de sus ciudadanos y empresas**.

IWA 48:2024 – Implementación de principios ambientales, sociales y de gobernanza (ESG)

En la actualidad, las organizaciones enfrentan una presión sin precedentes para integrar los factores **ambientales, sociales y de gobernanza (ESG)** en sus operaciones y estrategias corporativas. La **IWA 48:2024** surge como respuesta a esta necesidad, proporcionando un marco estandarizado desarrollado por la **Organización Internacional de Normalización (ISO)** que permite a las empresas implementar, gestionar y reportar sus prácticas ESG de manera efectiva y comparable a nivel global.

Este documento representa un avance significativo en el campo de la **sostenibilidad** corporativa, ya que establece un lenguaje común y principios claros que facilitan la integración de los ESG en la cultura organizacional.

A diferencia de otras normas ISO, la **IWA 48** no es certificable, pero su valor radica en su capacidad para orientar a las organizaciones en el desarrollo de sistemas de gestión ESG robustos y creíbles.

¿Qué es exactamente la IWA 48:2024?

La **International Workshop Agreement (IWA) 48:2024** es un acuerdo técnico que proporciona directrices prácticas para la implementación de principios ESG en organizaciones de cualquier tamaño y sector. Su objetivo principal es servir como puente entre los diversos marcos de reporting existentes (como **GRI, SASB y TCFD**) y las necesidades específicas de las empresas que buscan mejorar su desempeño en sostenibilidad.

El documento se estructura en tres pilares fundamentales:

- **Ambiental (E):** Aborda la gestión de recursos naturales, la reducción de emisiones, la economía circular y la adaptación al **cambio climático**.

- **Social (S):** Cubre aspectos como derechos humanos, condiciones laborales, diversidad e inclusión, y relación con las comunidades.

- **Gobernanza (G):** Incluye ética empresarial, gestión de riesgos, transparencia y estructura de gobierno corporativo.

La necesidad de estandarización en los reportes ESG

Uno de los mayores desafíos que enfrentan las organizaciones en materia de sostenibilidad es la proliferación de marcos y estándares de reporting ESG.

Administración de la calidad: 5 tendencias clave que marcarán 2025

2025 es el año en que el área de **administración de la calidad** asume el liderazgo en las empresas asistidas por la tecnología y la innovación. Los departamentos encargados de los **sistemas de gestión de calidad** serán determinantes en la toma de decisiones en la Alta Dirección y participarán en el diseño de las estrategias comerciales.

La administración de la calidad se integrará en todos los aspectos del negocio, **impulsada por la automatización de los sistemas de gestión, el uso de IoT** y, por supuesto, el posicionamiento definitivo de la Inteligencia Artificial.

Cuáles son las tendencias clave en administración de la calidad

Administración de la calidad retoma el liderazgo natural en la organización, y lo hace de la mano de la tecnología. La **automatización de los sistemas de gestión** marcó el trabajo en el área en 2024 y se

consolida en 2025. **Los aportes tecnológicos son los que definen las tendencias clave** en administración de la calidad:

1. IA autónoma y predictiva

2024 fue el año en que Inteligencia Artificial llegó al área de administración de la calidad, ayudando a escribir manuales de funciones y a gestionar documentos. 2025 es el año en el que **la IA dominará la gestión utilizando bots y sensores de IoT.**

El resultado es la posibilidad de recopilar datos de sensores en la planta de producción, generando análisis predictivos y utilizando agentes autónomos que realizarán tareas y tomarán decisiones sin intervención humana. Para ello, absorben información de otros sistemas de la organización y de las tareas diarias de los trabajadores. De esta forma, **se establecen patrones y entregan soluciones efectivas para mejorar la calidad y reducir la posibilidad de productos defectuosos**.

La IA generativa da paso en 2025 a los agentes de IA y el análisis predictivo. Los agentes de IA son sistemas autónomos que van un paso delante de la automatización, al prescindir del factor humano. La administración de la calidad utiliza estos agentes para **predecir problemas y gestionarlos antes de que se produzcan**.

2. Integración de HSE con la administración de la calidad

Las empresas entienden que no basta entregar productos de calidad. Los consumidores esperan que en la fabricación de esos productos **se adopten las mejores prácticas para proteger el medio ambiente, a los trabajadores y a la comunidad**.

Implementar un sistema de gestión de IA: componentes clave, retos y pasos a seguir

Implementar un sistema de gestión de IA es la vía para impulsar la innovación con base en Inteligencia Artificial, abordando los desafíos y los riesgos que se asocian a ella. Un SGIA basado en la norma **ISO 42001** permite a las empresas navegar con aceptable tranquilidad por las complejidades y los riesgos inherentes al uso de este desarrollo tecnológico, tratando de aprovechar al máximo todo su potencial.

La Inteligencia Artificial forma parte del día a día de un número cada vez mayor de empresas en todo el mundo. Empresas que ahora trabajan a marchas forzadas para implementar un sistema de gestión de IA. **Es importante conocer sus elementos clave** y los pasos necesarios para implementarlo.

Elementos clave que es preciso conocer para implementar un sistema de gestión de IA

Implementar un sistema de gestión de IA es, en sentido figurado, algo similar a armar una máquina. **Lo primero es identificar las partes que componen el sistema** y colocarlos en su lugar de acuerdo con su función. Esos componentes clave son los siguientes:

1. Gobernanza

La **gobernanza de la Inteligencia Artificial** es el elemento responsable de **garantizar la ética, la transparencia, la equidad y la inclusión**. En una sola palabra, la gobernanza representa justicia. Además, permite al sistema cumplir con los requisitos del estándar en el que se basa, que usualmente es ISO 42001.

2. Datos

Los resultados óptimos de un sistema de gestión provienen de la adecuada gestión de datos de buena calidad. Los datos íntegros, precisos, confiables y seguros **requieren protocolos estrictos de recopilación, etiquetado, procesamiento y almacenamiento**. Son requisitos ineludibles para el eficaz entrenamiento de un modelo de IA.

3. Gestión de riesgos

La razón principal para implementar un sistema de gestión de IA es tratar los riesgos asociados a la tecnología, con énfasis en la privacidad de datos, sesgos, derechos humanos, amenazas a la seguridad de las personas, etc. La **gestión de riesgos de la IA** es el eje principal del sistema.

IWA 48 vs. ISO 53001: principales diferencias

En 2025, las organizaciones enfrentan un desafío dual: **gestionar su impacto ESG (Ambiental, Social y Gobernanza)** y **alinearse con los Objetivos de Desarrollo Sostenible (ODS)** de la ONU. Para lograrlo, ISO ha desarrollado dos herramientas clave:

- **IWA 48:2024**: Guía práctica para implementar principios ESG (no certificable).
- **ISO 53001 (próxima a publicarse en 2025)**: Primera norma certificable para integrar los ODS en sistemas de gestión.

Aunque ambas comparten el objetivo de impulsar la sostenibilidad, sus enfoques, alcances y aplicaciones son distintos.

En este artículo, exploramos sus diferencias clave y cómo la herramienta **ISOTools** simplifica su implementación.

IWA 48 – La brújula ESG para la acción inmediata

Publicada en marzo de 2024, la **International Workshop Agreement 48 (IWA 48)** representa un hito en la estandarización de criterios **ESG** (Ambiental, Social y Gobernanza). Este documento técnico, desarrollado con aportes de más de 300 expertos de 42 países, ofrece una **guía práctica** para que organizaciones de todos los tamaños y sectores integren estos principios en sus operaciones. A diferencia de las normas ISO tradicionales, la **IWA 48 no es certificable**, pero su valor radica en proporcionar un marco **flexible y adaptable** que evita la burocracia excesiva.

El corazón de la IWA 48 late en sus **tres pilares fundamentales**. El componente **ambiental (E)** aborda aspectos como la gestión de recursos naturales, la economía circular y la adaptación al cambio climático. El pilar **social (S)** cubre temas sensibles como derechos humanos, condiciones laborales y relación con comunidades. Finalmente, la **gobernanza (G)** se enfoca en ética empresarial, transparencia y estructura corporativa. Lo innovador de este documento es su **enfoque práctico**, que incluye herramientas listas para usar como **matrices de materialidad** y **protocolos anti-greenwashing**.

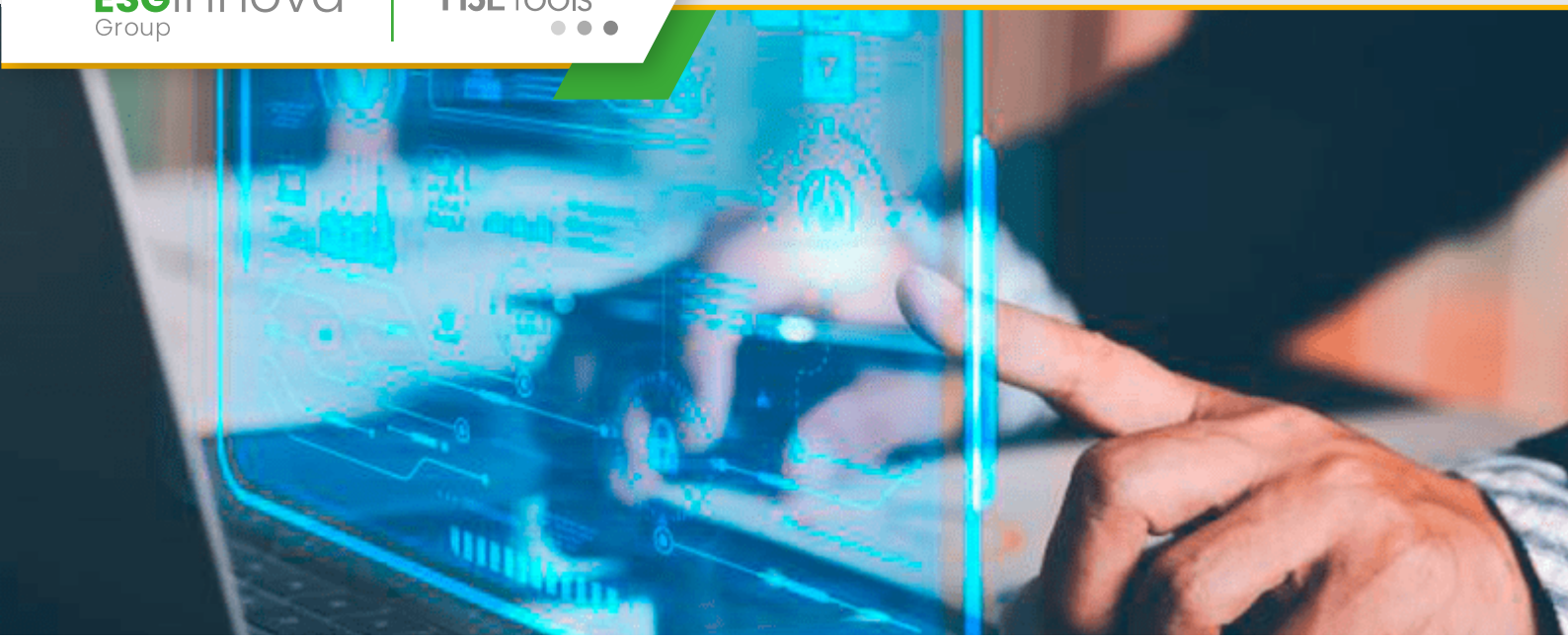
ISO 53001 – El sistema de gestión para los ODS

Mientras la IWA 48 se centra en ESG, la futura **ISO 53001** (cuyo borrador final está previsto para junio de 2025) representa un avance cualitativo al ofrecer el primer **sistema de gestión certificable** alineado con los **Objetivos de Desarrollo Sostenible (ODS)** de la ONU. Esta norma sigue la **Estructura de Alto Nivel (HLS)** característica de las normas ISO, lo que facilita su integración con otros sistemas de gestión existentes.

ESGinnova
Group

HSE Tools

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



Cómo elegir el mejor Software HSE: factores clave a considerar

El mejor Software HSE es siempre **una herramienta predictiva, fácil de utilizar y que cumple funciones de gestión de riesgos, pero también administrativas**. Además de todo ello, debe crecer con la empresa, entregar canales de comunicación fluidos y efectivos y, sobre todo, tener capacidad para generar cultura HSE, confianza en las partes interesadas y **mejora continua de la gestión**.

Cómo elegir el mejor Software HSE

Ante una oferta de productos amplia, la elección del mejor Software HSE puede ser una tarea abrumadora. Las organizaciones necesitan evaluar, de forma prioritaria, **cuatro criterios básicos para acertar en la elección.**

1. Adaptabilidad a las necesidades y la complejidad de la organización

El software se adaptará a las necesidades de la organización siempre que **entregue las funcionalidades para resolver problemas actuales y futuros**. Si la organización tiene dificultades para gestionar sus documentos, esta es una característica esencial en el checklist de selección. Si la organización no trabaja con contratistas ahora, pero tiene proyectado hacerlo, es importante que el **software para control de contratistas** sea uno de los módulos disponibles, para poder incorporarlo cuando sea necesario.

2. Funcionalidades y eficiencia de los módulos

Las empresas que buscan el mejor Software HSE valoran especialmente que la solución sea modular. Es esencial analizar cada uno de esos módulos y **comprobar si ofrece las funcionalidades apropiadas.** Pasar del primer nivel para investigar un poco más a fondo es una buena decisión. Los proveedores que entregan módulos eficaces y con funcionalidades relevantes no tienen restricciones en demostrarlo ante sus posibles clientes.

3. Respaldo y capacidad de crecimiento con la organización

Un Software de Gestión HSE no es un producto para unos meses. Las organizaciones mutan, crecen y se diversifican. El marco regulatorio también experimenta transformaciones importantes. Por eso, es esencial verificar la capacidad que tienen el software, el proveedor y sus aliados estratégicos para **acompañar a la empresa en su recorrido sin que las partes interesadas se vean afectadas**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Plataforma de gestión HSE: clave para gestionar operaciones en múltiples sitios

Las organizaciones que tienen sucursales o que operan en lugares diversos se enfrentan a un gran desafío a la hora de gestionar la seguridad y el cumplimiento de las normas de seguridad laboral y ambiental. Una **plataforma de gestión HSE** se convierte en una herramienta imprescindible para optimizar la **gestión de documentos y registros**, fundamental para asegurar el cumplimiento.

Una plataforma de gestión HSE **ayuda a las empresas a asumir un enfoque coherente y estandarizado**. Esto significa que, aun con obligaciones de cumplimiento diferentes y entornos culturales, regulatorios y sociales diferentes, la gestión se basa en unos postulados y en unos ejes de gobernanza únicos. La palabra clave es centralización.

Desafíos que debe afrontar una plataforma de gestión HSE para múltiples sitios

Cuando la gestión necesita tratar problemas, riesgos y personas en ubicaciones a veces muy alejadas unas de otras, surgen problemas que no son fáciles de resolver sin la ayuda de una plataforma de gestión HSE. El trabajo para una herramienta tecnológica de esta naturaleza es arduo, puesto que **es necesario enfrentar obstáculos de alta complejidad**. Algunos de ellos son los siguientes:

1. Diversidad de marcos regulatorios

Incluso dentro del mismo país, las normas y leyes son diferentes. En el área ambiental, además, las condiciones bioclimáticas tienen relevancia en las obligaciones de cumplimiento. Garantizar el **cumplimiento normativo** y regulatorio es el primer desafío que debe superar la plataforma de gestión HSE.

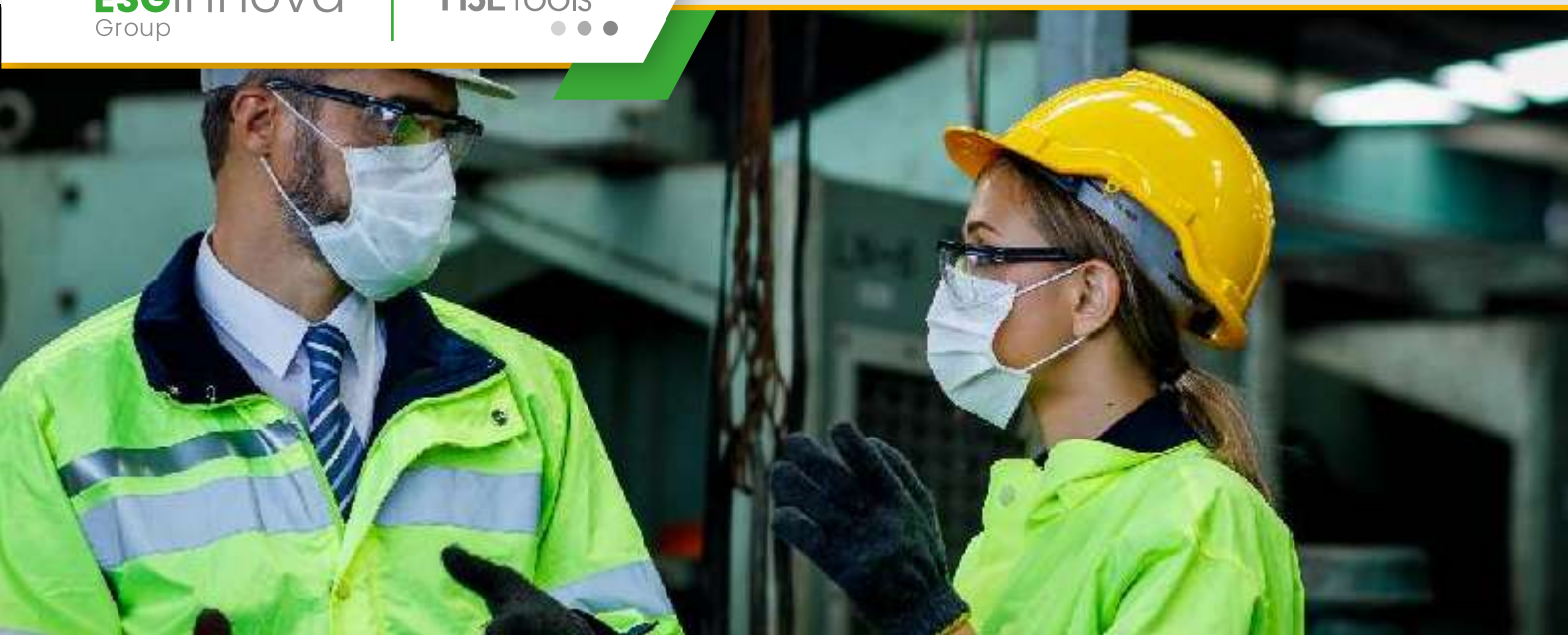
2. Protocolos, prácticas y estándares de seguridad diversos

Los trabajadores de una misma empresa que trabajan en ubicaciones diferentes pueden caer en el error de crear sus propias normas y apartarse de lo determinado por el equipo de HSE central. Las directrices, las prácticas, el uso de **equipos de protección en el lugar de trabajo**, además de los requisitos de capacitación, **necesitan guardan un nivel de coherencia aceptable que permita auditar y revisar la gestión** sobre parámetros similares.

3. Formación de silos de datos

Uno de los beneficios más interesantes que ofrece una plataforma de gestión HSE es la **centralización de la información.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Qué se entiende por seguridad industrial?

La **seguridad industrial** se desarrolla como la garantía de protección de los trabajadores de cualquier organización, haciendo más efectiva la operatividad y el cuidado del medio ambiente. Los riesgos laborales cobran cada vez más importancia dentro de la planificación empresarial, y esto es debido a los **derechos** que los **trabajadores** han ido obteniendo a lo largo de los años. La fuerza laboral que ejercen los profesionales está estrechamente vinculada a su valía, y a ser actores imprescindibles en el desarrollo de la actividad diaria. Si a esto le sumamos los desafíos ambientales cada vez más complejos a los que se enfrenta la humanidad, se necesita dar una vuelta al enfoque y a las herramientas que se utilizan para mantenerse a la vanguardia.

Por ello, vamos a desarrollar este concepto ligado a las últimas tendencias en el ámbito de la **Salud, Seguridad y Medio Ambiente (HSE)**, y cómo las soluciones tecnológicas son sin duda el futuro para transformar la manera en que las empresas abordan estos desafíos.

¿Qué es la seguridad industrial?

La seguridad industrial es un **conjunto de prácticas, normas y procedimientos diseñados para prevenir accidentes, enfermedades laborales y daños ambientales en entornos industriales**. Su objetivo principal es crear un entorno de trabajo seguro, saludable y sostenible, protegiendo tanto a los empleados como a las instalaciones y el medio ambiente.

Elementos clave de la seguridad industrial:

01. **Prevención de riesgos**: Identificar y evaluar peligros potenciales, como maquinaria pesada, sustancias químicas o condiciones inseguras.

02. **Cumplimiento normativo**: Adherirse a leyes y estándares internacionales, como las normas ISO 45001 (seguridad laboral) e ISO 14001 (gestión ambiental).

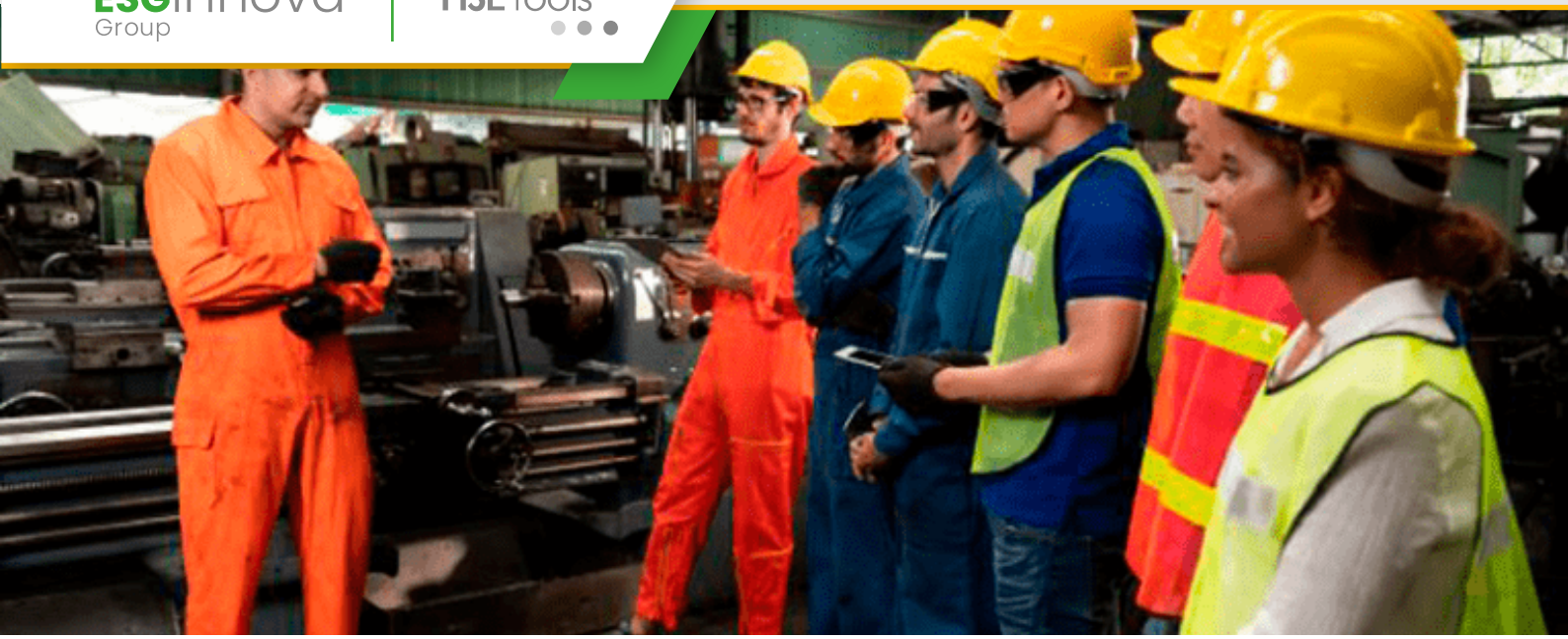
03. **Equipos de protección personal (EPP)**: Proporcionar a los trabajadores herramientas como cascos, guantes y mascarillas para minimizar riesgos.

04. **Capacitación continua**: Formar a los empleados en prácticas seguras y protocolos de emergencia.

05. **Gestión de emergencias**: Contar con planes de acción para situaciones críticas, como incendios o derrames químicos.

El sector HSE está evolucionando rápidamente, impulsado por la **tecnología** y la creciente conciencia sobre la importancia de la **sostenibilidad**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Involucrar a los contratistas en la capacitación en seguridad: 10 estrategias efectivas

La **capacitación en seguridad** es una cuestión crítica en la **gestión de contratistas**. Integrarla puede resultar complejo cuando se trata de trabajos estacionales, cuando esos terceros desempeñan su labor en diferentes localizaciones o en casos en los que es necesario desarrollar un proyecto con cierta premura.

En cualquiera de las circunstancias, no existe razón válida para pasar por alto la capacitación en seguridad al trabajar con contratistas. Por eso, es importante **diseñar estrategias para integrar a la fuerza laboral externa en todos los procesos de seguridad y salud en el trabajo** que se aplican para los empleados directos.

Cómo involucrar a los contratistas en la capacitación en seguridad

Accidentes, lesiones o cualquier afectación a la integridad de contratistas acarrea los mismos riesgos para la organización que si los sufren empleados directos. Estos riesgos son sanciones, multas, incremento de las pólizas de seguros e, incluso, cierre de la operación. Por eso, **es importante trabajar en estrategias eficaces para integrar a los contratistas en la capacitación en seguridad**. Las siguientes son diez formas efectivas para hacerlo:

1. Identificar la causa raíz del problema

Analizar los desafíos a los que se enfrentan los contratistas es el punto de partida para identificar qué dificulta la capacitación en seguridad. Después será necesario proponer una solución. En el caso de los trabajadores que están dispersos en ubicaciones remotas, la capacitación virtual es la solución. Si se trata de reticencia injustificada del contratista, es preciso incluir la capacitación en los requisitos contractuales. Cada causa es susceptible de ser tratada y eliminada. Finalmente, **es importante que cada contratista reciba la capacitación adecuada**. Los que trabajan en alturas, los que trabajan en confinamiento, los que están expuestos a temperaturas extremas, etc.

2. Establecer la capacitación como una obligación y comunicar sus beneficios

La capacitación es un beneficio para las dos partes. Es importante que los contratistas lo entiendan, y eso se logra con comunicación empática y asertiva.

Software de cumplimiento HSE: cómo solucionar los mayores desafíos ambientales y de seguridad

El **software de cumplimiento HSE** es la herramienta más efectiva con la que cuentan los profesionales en esta área para afrontar con éxito los múltiples retos que plantea la **gestión HSE**. Desafíos tan complejos como el dinamismo del marco regulatorio, las dificultades para crear cultura de seguridad o la necesidad de obtener información en tiempo real no se pueden afrontar utilizando documentos en papel u hojas de cálculo

Emplear procesos obsoletos o manuales entraña riesgos de cumplimiento. Es preciso contar con un software de cumplimiento HSE eficaz y avanzado, diseñado para **automatizar los procesos clave de la gestión** y mejorar la precisión de los datos, con el objetivo de contar con información en tiempo real que ayude a las organizaciones a tomar decisiones bien informadas.

Desafíos de seguridad y ambientales que es posible superar con un software de cumplimiento HSE

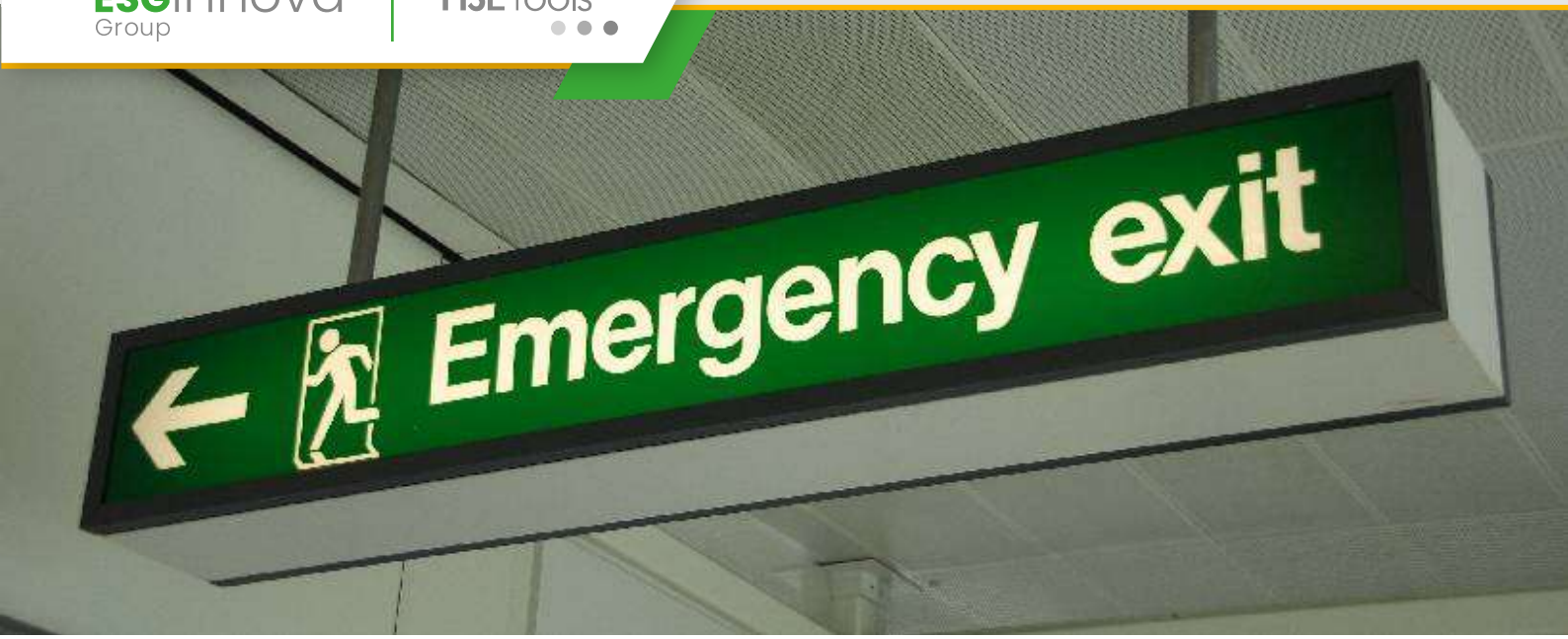
Gestión ambiental y gestión de seguridad y salud en el trabajo son las **áreas que concentran la mayor proporción de obligaciones de cumplimiento** en una organización. Solo por eso, la automatización con base en un software de cumplimiento HSE tendría que ser una decisión estratégica indiscutible. No obstante, si se buscan más argumentos, es posible revisar la lista de desafíos que se pueden superar gracias a la automatización:

1. Dinamismo del marco regulatorio

El dinamismo que muestra el marco regulatorio en las áreas comprometidas en la gestión HSE no tiene punto de comparación con otro campo en una organización típica. **Garantizar el cumplimiento en un escenario tan volátil no es fácil** y aún es más complicado si se incluyen múltiples ubicaciones. Más allá del universo de normas y leyes siempre cambiantes, es preciso considerar que **la empresa debe preocuparse por las obligaciones de cumplimiento locales, las nacionales y las internacionales**. Y para cada una de ellas debe resolver el problema mismo que plantea la obligación, la documentación, la actualización sobre la evolución de la obligación y las necesidades de **capacitación en seguridad** en muchos lugares, para asegurar que los empleados indicados sepan lo que deben hacer.

Cómo lo soluciona un software de cumplimiento HSE

Los problemas asociados son dos: imposibilidad de mantenerse al día y dificultad para hacer seguimiento a un enorme número de tareas para satisfacer los requisitos de las obligaciones.



¿Cómo se establece una ruta de evacuación en una empresa?

En el ámbito de la **Salud, Seguridad y Medio Ambiente (HSE)**, la seguridad de las personas es una prioridad absoluta. En este sentido, establecer una **ruta de evacuación eficiente** dentro de una empresa en el contexto de una **emergencia**, además de ser un requisito legal, es también una responsabilidad ética que puede salvar vidas.

Para ello vamos a enfocarnos en desarrollar cómo se establece una ruta de evacuación. En las siguientes líneas encontrarás las **últimas tendencias, consejos prácticos y soluciones innovadoras** que se encargan de diseñar e implementar rutas de evacuación efectivas, con un enfoque especial en cómo la **transformación digital** está revolucionando la gestión de la seguridad empresarial.

¿Qué es y cómo se establece una ruta de evacuación?

Las **rutas de evacuación** son trayectos diseñados para guiar a las personas desde el interior de un edificio hacia un lugar seguro en caso de emergencia, como incendios, terremotos o fugas de sustancias peligrosas. Su principal objetivo es facilitar una evacuación rápida, ordenada y segura, minimizando el riesgo de lesiones o pérdidas humanas.

En un entorno empresarial, donde pueden convivir cientos o miles de personas, contar con rutas de evacuación bien planificadas es crucial. Además de proteger a los empleados, también ayudan a salvaguardar los bienes materiales y a cumplir con las normativas de seguridad vigentes.

Elementos clave de una ruta de evacuación efectiva

Para que una ruta de evacuación cumpla su función, debe estar compuesta por tres elementos principales:

- **Acceso a la ruta de salida**: Es el camino que conecta cualquier área del edificio con la ruta de evacuación principal. Debe estar libre de obstáculos y claramente señalizado.

- **Ruta de salida**: Es el recorrido protegido y aislado que conduce hacia las salidas de emergencia. Debe estar diseñado para evitar zonas de riesgo, como áreas con maquinaria pesada o materiales inflamables.

- **Descarga de salida**: Es el punto final de la ruta, que lleva a un **área segura** fuera del edificio, como un punto de reunión predefinido.

Seguridad del contratista: cómo superar las brechas de cumplimiento en el lugar de trabajo actual

Una **gestión de contratistas** eficaz es clave para el cumplimiento regulatorio, legal y normativo. Dentro de ella, hay un apartado de especial relevancia: la **seguridad del contratista**. Reviste tanta importancia como los esfuerzos que se hacen para velar por la integridad de los empleados de la empresa, sin embargo, afronta desafíos únicos que la convierten en una tarea compleja.

Los contratistas pueden trabajar en ubicaciones muy diversas y en muchas ocasiones son itinerantes. Es un cuerpo heterogéneo que muestra **diferentes niveles de cultura de seguridad, de formación, capacitación y concienciación**. Todo se refleja en una disparidad de necesidades y expectativas en cada uno de ellos.

Por qué es importante la seguridad del contratista

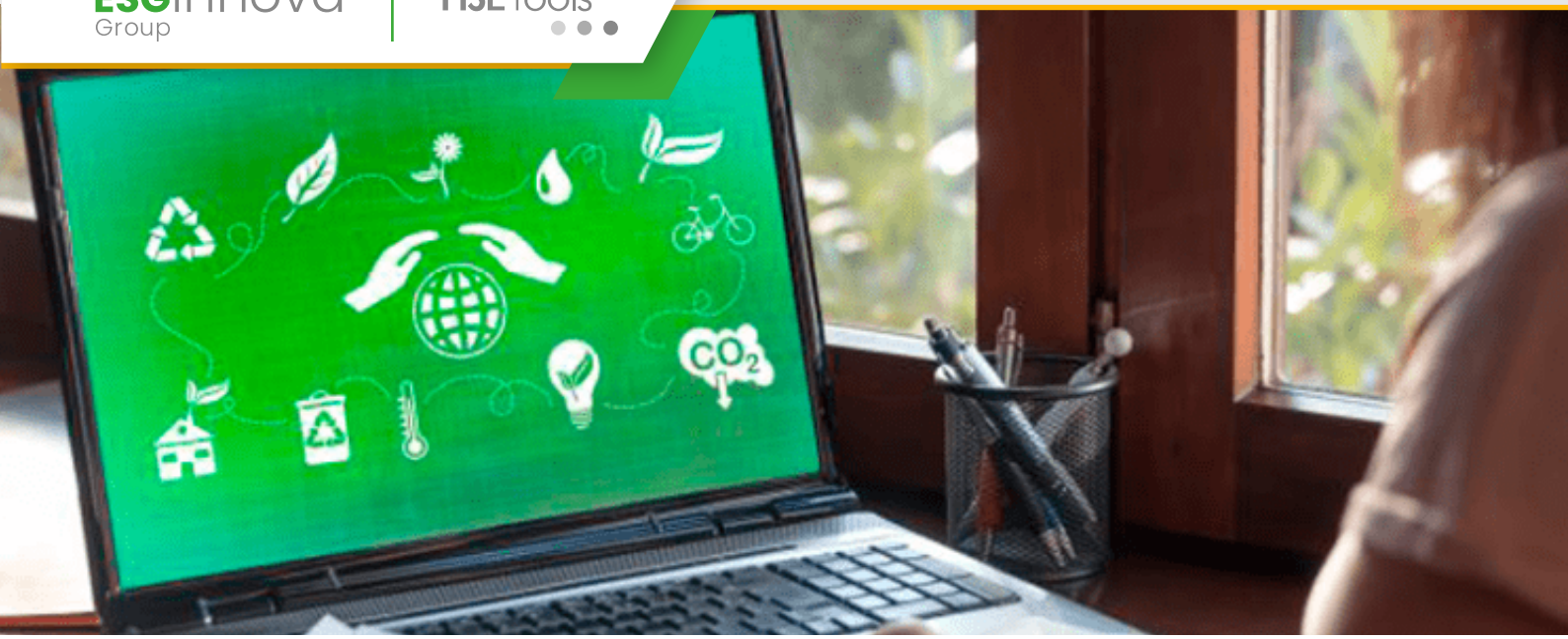
Los contratistas **aportan habilidades técnicas y recursos operativos estratégicos** para el desarrollo de proyectos vitales para las organizaciones. La flexibilidad, la movilidad y la diversidad de especialidades suponen una contribución significativa para el crecimiento y el éxito de las empresas que hacen uso de esta fuerza laboral externa.

Las características que hacen tan funcionales y atractivos a los contratistas, de forma paradójica, son las que complican la tarea de ofrecerles condiciones de seguridad y salud óptimas. Por eso, es esencial **contar con personas y recursos de toda índole, incluyendo los tecnológicos**, para gestionar la seguridad del contratista.

Es necesario destacar la importancia de asegurar el **cumplimiento normativo de HSE** en todos sus aspectos. La gestión de seguridad del contratista representa un desafío, pero no es menos importante que la seguridad de los empleados. Ambas generan obligaciones de cumplimiento y **es preciso verificar que no existan brechas** que pueden representar costes muy altos, parálisis de un proyecto o, incluso, la pérdida de una licencia.

Cumplir con normas y exigencias de seguridad y salud en el trabajo es una obligación de la organización que no excluye a los contratistas. La empresa es responsable de su bienestar tanto como lo es del de sus empleados. Entender y aplicar este principio **evita riesgos, litigios judiciales, sobrecostes de operación, sanciones y menoscabo de la reputación.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo una aplicación HSE puede transformar la estrategia de sostenibilidad

Una **aplicación HSE** es un elemento común en las empresas modernas. Una **plataforma de gestión HSE** es una herramienta capaz de recopilar datos de forma autónoma, automatizar tareas, mejorar procesos, crear flujos de trabajo eficientes y contribuir con todo ello a garantizar el cumplimiento regulatorio y normativo.

Una aplicación HSE, además, tiene capacidad para transformar y **potenciar una estrategia de sostenibilidad en una organización de cualquier tamaño** o cualquier industria. Para entender cómo lo consigue, el primer paso es conocer qué son los aspectos e impactos ambientales y por qué es importante que las empresas reconozcan los suyos.

Qué son los aspectos e impactos ambientales

Los aspectos ambientales son actividades, procesos, servicios o productos de una organización que interactúan con el medio ambiente.

Un proceso que genere residuos, que produzca emisiones o que requiera consumo de recursos naturales o energéticos es un aspecto ambiental.

Por otra parte, **los impactos ambientales son las alteraciones que producen los aspectos** en el entorno, en los recursos naturales o en el medio ambiente. Los impactos, no obstante, pueden ser positivos o negativos. El primer paso para iniciar un sistema de gestión HSE es identificar los **aspectos e impactos ambientales**, para lo cual **es preciso revisar todas las actividades, todos los procesos**, las líneas de producción o los procedimientos asociados a la prestación de un servicio. Algunas actividades o procesos no están relacionados con el producto o servicio que entrega la organización, **es el caso de las actividades administrativas o los procesos que buscan garantizar la confortabilidad en las instalaciones**. Los sistemas de aire acondicionado, calefacción o refrigeración, por ejemplo, pueden requerir el uso de combustibles, de fuentes de energía no renovables o de refrigerantes, entre otros elementos que son impactos ambientales.

¿Es necesario tener un sistema de gestión para aprovechar los beneficios de una aplicación HSE?

No es obligatorio, pero lo cierto es que aporta muchos beneficios. Para entenderlo hay que partir desde la base: **la gestión HSE incorpora tres elementos: salud, seguridad y medio ambiente.** Así, **la organización tendría que contar con dos sistemas de gestión**: uno de seguridad y salud en el trabajo, **ISO 45001**, y otro de gestión medioambiental, ISO 14001. O, como una alternativa, tener un sistema integrado que, de ser posible, agregue la gestión de la calidad (ISO 9001) Un sistema de gestión, integrado o no, **ayuda a optimizar recursos y a lograr objetivos de forma sistemática**, siempre apuntando a la mejora continua.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué es el analisis de Pareto?

¿Cómo esta herramienta puede transformar la **gestión de riesgos** en torno a la Salud, Seguridad y Medio Ambiente (HSE) en tu empresa? El **análisis de Pareto** es un método basado en el famoso **Principio 80/20**, además de permitir identificar los problemas más críticos, también prioriza acciones para maximizar el impacto en áreas como la **Salud, Seguridad y Medio Ambiente (HSE)**.

Pero, ¿cómo aplicarlo en el ámbito empresarial? En el siguiente desarrollo encontrarás las claves para ello, y cómo nuestra plataforma **HSETools** puede ayudarte a implementarlo de manera eficiente para mejorar la gestión de riesgos y fomentar un entorno laboral más seguro y sostenible.

¿Qué es el Análisis de Pareto?

El analisis de Pareto es una técnica que permite **identificar y priorizar los factores que generan el mayor impacto en un conjunto de datos**. Su nombre proviene del economista italiano **Vilfredo Pareto**, quien observó que el 80% de la riqueza en Italia estaba concentrada en el 20% de la población.

Este principio se ha extrapolado a múltiples disciplinas, incluyendo la gestión de calidad, los negocios y, por supuesto, la gestión de HSE.

En términos prácticos, el análisis de Pareto ayuda a responder preguntas como:

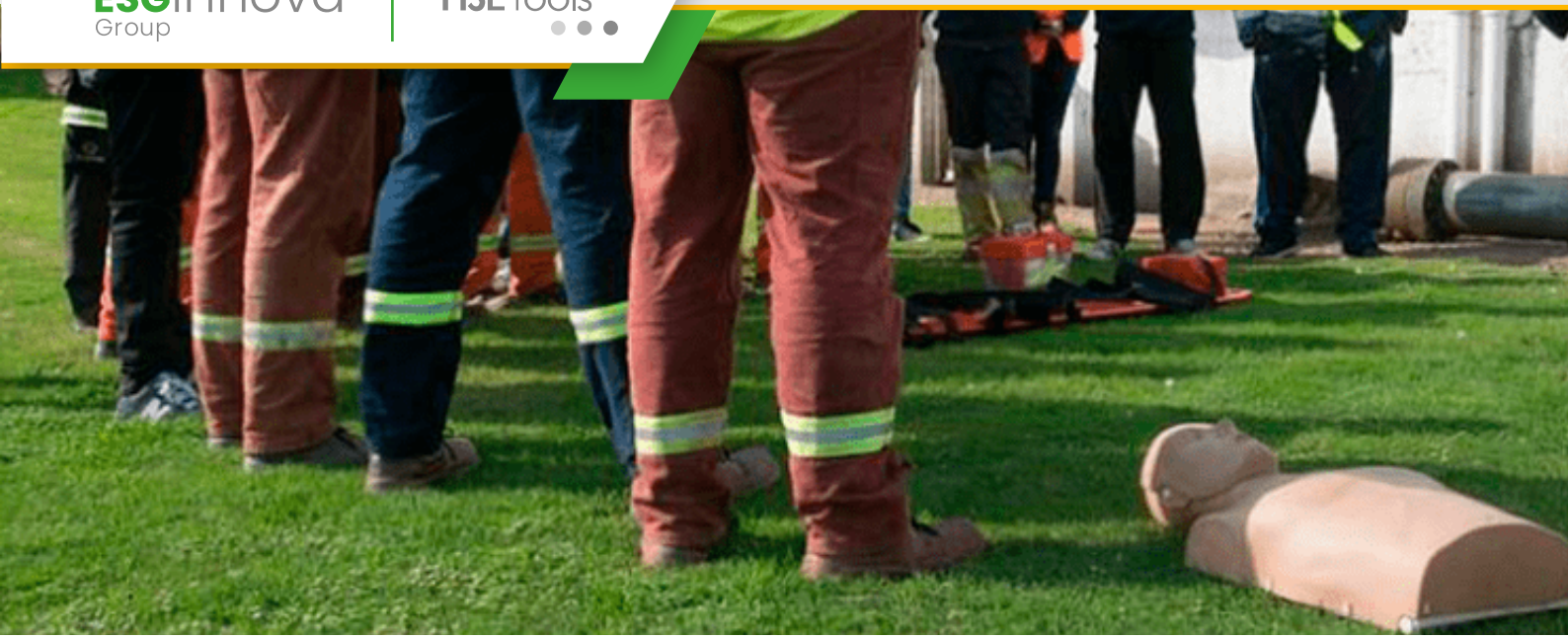
- ¿Cuáles son las **causas principales de accidentes laborales** en mi empresa?
- ¿Qué factores están generando el **mayor impacto ambiental**?
- ¿Dónde deberíamos enfocar nuestros **recursos** para mejorar la **seguridad** y el **bienestar** de nuestros empleados?

Cómo aplicar el Analisis de Pareto en el sector empresarial

En el ámbito empresarial, el análisis de Pareto es una herramienta poderosa para **optimizar recursos y mejorar la eficiencia**. Aquí te explicamos cómo puedes aplicarlo en la gestión de HSE:

01. Identificar problemas críticos

- Recopila datos sobre incidentes, riesgos o no conformidades en tu empresa. Por ejemplo, si estás analizando accidentes laborales, clasifica las causas (caídas, manejo de maquinaria, exposición a sustancias peligrosas, etc.).



Capacitación en seguridad laboral: 5 razones por las que actualización es cada vez más importante

La **capacitación en seguridad laboral** es una etapa ineludible en la selección, incorporación y **gestión de contratistas**. Es un requisito esencial porque de él depende en gran medida la seguridad de la fuerza laboral externa, la de los empleados que interactúan con terceros, el cumplimiento de las obligaciones regulatorias y normativas de la organización y el desarrollo de un contrato en condiciones adecuadas y productivas.

En algunas organizaciones, el número de trabajadores externos supera al de empleados directos. Para este tipo de empresas, en las que **suele producirse una rotación alta de este tipo de trabajadores**, el principal reto está en mantener la actualidad de la capacitación en seguridad laboral. En muchas ocasiones la capacitación pierde vigencia porque el contratista **asume funciones o puestos de trabajo que requieren nuevos contenidos**.

En algunos casos, la incorporación de tecnología, máquinas, o la simple modificación de un proceso puede conducir a la necesidad de renovar la capacitación en seguridad.

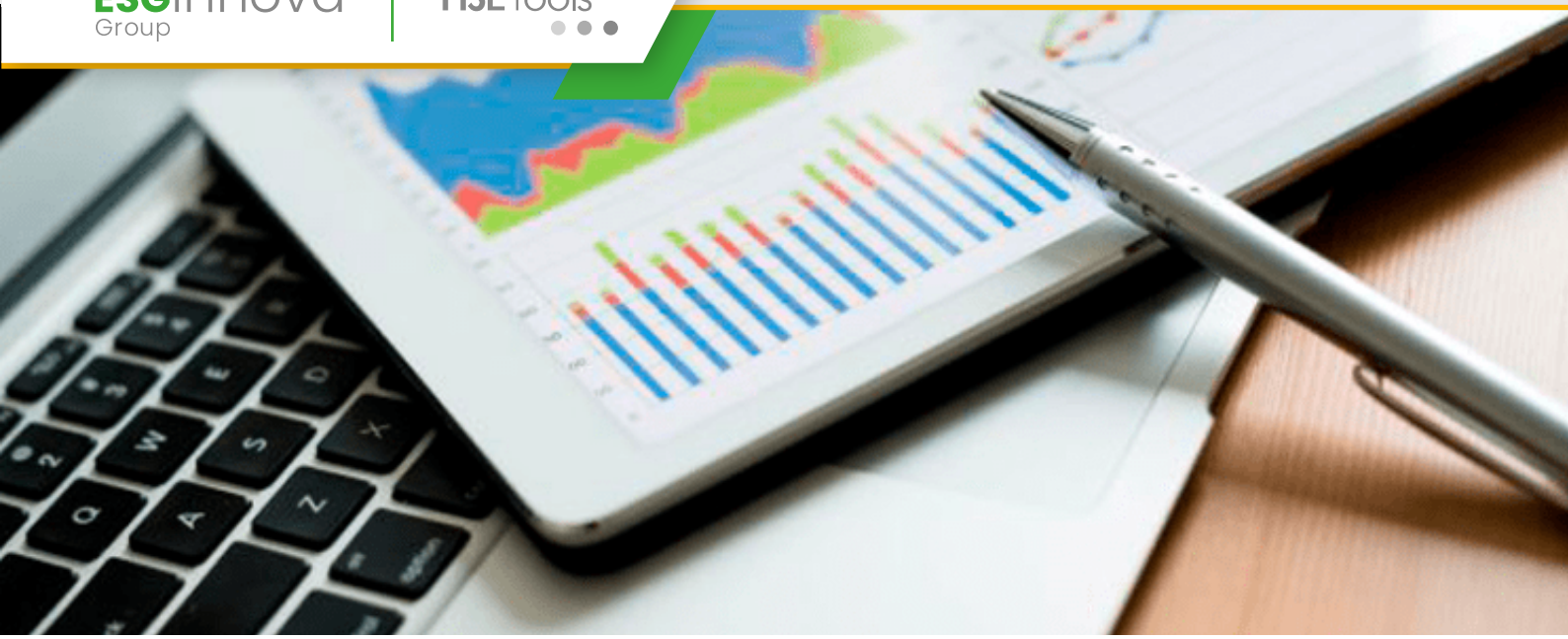
Por qué es importante actualizar la capacitación en seguridad laboral

Una razón para mantener actualizada la capacitación en seguridad laboral de los contratistas es la que indica el sentido común: las empresas que reciclan sus programas de capacitación en seguridad laboral **experimentan menos incidentes y menos accidentes**. La tasa desciende hasta en un 50 %, aunque hay otros motivos para ello.

1. Los contratistas tienen una tasa de rotación muy alta

Una de las características que hace que los contratistas sean tan funcionales y atractivos para muchas empresas es también la condición que genera un nivel mayor de riesgo: su **capacidad de movilidad y adaptabilidad**. El problema es que las actividades que realizan no siempre se programan con la suficiente anticipación. Sin una actualización de la capacitación en seguridad laboral, **la probabilidad de ocurrencia de un accidente se incrementa de forma exponencial**.

Temas como **trabajos verticales y en altura**, en profundidad o en aislamiento, así como la operación segura de maquinaria pesada, entre otros temas recurrentes en las organizaciones que trabajan con contratistas, **necesitan actualización rutinaria cada vez que se inicia un nuevo contrato**.



Cómo superar los retos de cumplimiento ambiental con una herramienta software HSE

El **cumplimiento ambiental** es una preocupación de primer orden para la Alta Dirección de cualquier organización, junto a la ciberseguridad, las finanzas y la seguridad de los empleados. Es por ello que ocupa un lugar relevante dentro de los **planes de acción HSE**.

El interés que manifiestan las organizaciones en el cumplimiento ambiental es proporcional a los desafíos que entraña garantizar que la empresa cumpla con las normativas y las regulaciones ambientales. Sin obviar, por supuesto, que **la ausencia de cumplimiento ambiental implica problemas penales, financieros y reputacionales**. Por todo ello, las empresas necesitan utilizar todos los recursos a su alcance para superar los retos de cumplimiento ambiental, y **una de las herramientas que han demostrado mayor eficiencia es el software HSE**.

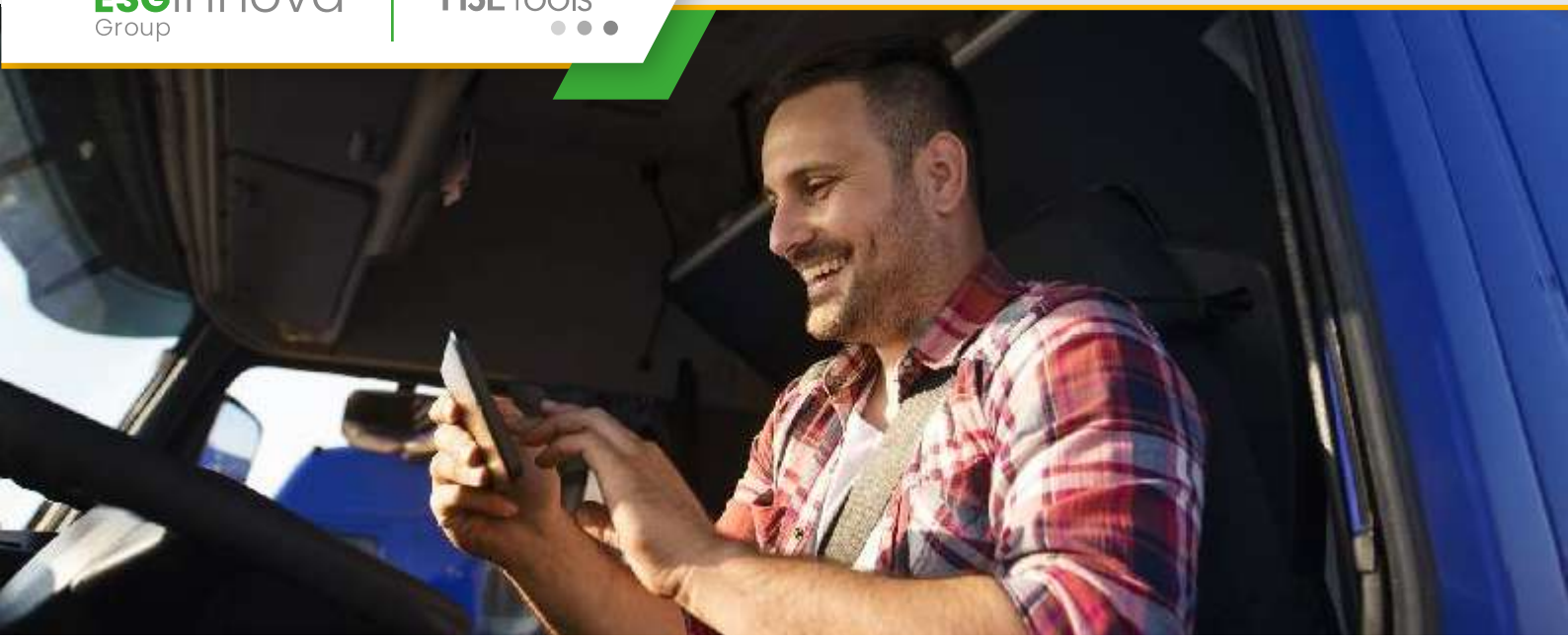
Cómo puede un software HSE ayudar a afrontar los desafíos del cumplimiento ambiental

La tecnología entrega aplicaciones y soluciones innovadoras, que resuelven muchos de los retos a los que se enfrentan las organizaciones, incluidos los que pueden afectar al cumplimiento ambiental. En esta área en particular, una **aplicación HSE puede ayudar a una empresa a afrontar desafíos de formas muy diferentes**:

1. Monitorea el espectro normativo y regulatorio

Las obligaciones en el área ambiental tienen diferentes orígenes: leyes, decretos, normativas, directivas, acuerdos con la comunidad, compromisos contractuales, etc. Algunas son de orden local, otras son regionales o nacionales y algunas de alcance internacional. La diversidad es ya un problema, pero si **a ello se suma la volatilidad o dinamismo**, se llega a la conclusión de que la única forma de mantener el control es asignar a un equipo de varias personas la labor de monitorear la evolución de las obligaciones de cumplimiento ambiental, la aparición de nuevas normas o la extinción de otras. El conocimiento regulatorio y normativo no resuelve el problema del todo. Queda pensar en que cada obligación de cumplimiento ambiental requiere realizar acciones, recopilar datos y presentar informes. El cumplimiento de estos requisitos **puede demandar conocimiento, recursos tecnológicos o físicos** y tiempo para hacer lo que sea necesario. El **software de cumplimiento HSE realiza un monitoreo constante de las principales fuentes de noticias sobre cambios en el marco regulatorio o normativo**. También puede almacenar un inventario de obligaciones de cumplimiento y crear flujos de trabajo automáticos, notificando la asignación de tareas a cada empleado responsable y alertando sobre el retraso o el incumplimiento.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



5 claves para llevar a cabo la prevencion de accidentes in itínere

Los **accidentes in itínere**, definidos como aquellos que ocurren durante el desplazamiento habitual entre el domicilio del trabajador y su lugar de trabajo, representan uno de los mayores retos en la **gestión de la seguridad y salud laboral**. Según datos de la **Organización Internacional del Trabajo (OIT)**, este tipo de accidentes constituye aproximadamente el **15% del total de accidentes laborales** registrados anualmente, con consecuencias significativas tanto para los trabajadores como para las organizaciones.

Un desafío prioritario en seguridad laboral

Para las empresas, estos incidentes generan **costes directos** (indemnizaciones, bajas laborales) e **indirectos** (pérdida de productividad, daño reputacional). Además, en muchos países, los accidentes in itínere tienen la misma consideración legal que los accidentes ocurridos en el puesto de trabajo, lo que exige a las organizaciones implementar **estrategias preventivas eficaces**.

En este artículo, analizaremos en profundidad **cinco claves fundamentales** para prevenir estos accidentes, incorporando las **últimas tendencias en prevencion de accidentes en riesgos laborales** y destacando cómo herramientas tecnológicas como el **Software de Gestión de Riesgos de HSETools** pueden transformar la seguridad en los desplazamientos laborales.

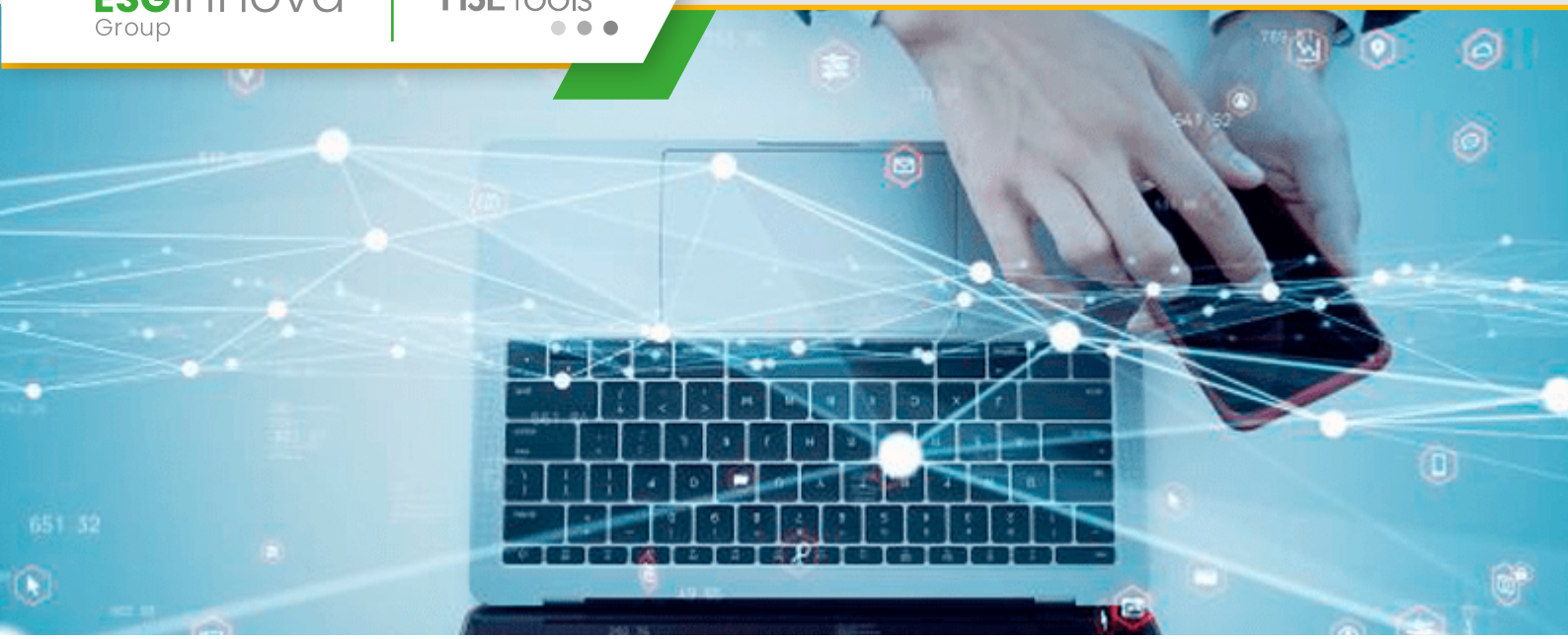
1. Fomentar una cultura de prevencion de accidentes con formación continua

La **concienciación y formación** de los empleados es el pilar básico para reducir los accidentes in itínere. Muchos de estos siniestros están relacionados con **distracciones al volante**, **fatiga acumulada** o **desconocimiento de técnicas de conducción segura**. Por ello, las empresas deben desarrollar **programas formativos completos** que aborden estos riesgos de manera específica.

Una de las **tendencias más innovadoras** en este ámbito es el **microlearning**, un método de aprendizaje basado en contenidos breves y accesibles desde dispositivos móviles. Este enfoque permite a los trabajadores adquirir conocimientos sobre **seguridad vial** sin sobrecargar su jornada laboral. Los temas clave deben incluir:

- **Planificación de rutas seguras**
- **Gestión de la fatiga en la conducción**
- **Prevención de distracciones (móvil, GPS, etc.)**
- **Conducción en condiciones meteorológicas adversas**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Gestión de riesgos de los contratistas: razones para utilizar soluciones digitales

La **gestión de riesgos de los contratistas** se ocupa de identificar, evaluar, categorizar, priorizar, eliminar o mitigar el impacto de las amenazas asociadas al uso de fuerza laboral externa. La dependencia creciente de terceros por parte de muchas organizaciones hace que la **gestión de contratistas** sea clave dentro de sus políticas HSE.

La gestión de riesgos de los contratistas es un área que no solo protege a los trabajadores contratados bajo esta modalidad. También la empresa elimina o **previene riesgos de cumplimiento, de seguridad y salud en el trabajo y de seguridad de la información**, entre otros, que de no hacerlo le resultarían muy costosos.

Por qué es importante la gestión de riesgos de los contratistas

Los contratistas están expuestos a muchas eventualidades. Los **riesgos de seguridad y salud en el trabajo**, ocupan el primer

lugar. En algunos casos, **existen riesgos particulares que se asocian a esa modalidad de contratación.** Se trata de riesgos que no solo amenazan la integridad del trabajador. **Ponen en peligro la relación con todos los trabajadores, la reputación de la organización, el futuro del proyecto** en el que se emplean contratistas y, por supuesto, los costes financieros ocasionados por multas, sanciones o pérdida de licencias. Por eso es tan importante la gestión de riesgos de los contratistas. Y por eso es necesario, antes de abordar de las razones para **digitalizar la gestión**, hacer un repaso por los riesgos específicos que se asocian a esta fuerza laboral.

Amenazas específicas que aborda la gestión de riesgos de los contratistas

Las organizaciones utilizan contratistas como una estrategia que les hace ganar competitividad. Los contratistas **aportan conocimientos, habilidades y experiencia** que la organización requiere para ejecutar un proyecto de alto valor. Tampoco hay que olvidar la facilidad de movilidad y translación de esta fuerza laboral, que representa una gran oportunidad para la empresa. Las oportunidades y beneficios son muchos, pero **existen riesgos que es preciso tratar** para aprovecharlos:

- **Cumplimiento**: los contratistas pueden utilizar procedimientos o protocolos diferentes. Estas diferencias pueden causar **brechas de cumplimiento** o riesgos para los trabajadores y para la organización, que podría incurrir en multas o sanciones.

- **Fallos y problemas por falta de conocimiento y experiencia**: sucede especialmente en lo relacionado con normas internas de la organización.

Normativa europea unificada acerca de la calidad del aire

Los **estándares de calidad del aire** han dejado de ser una mera recomendación para convertirse en un requisito fundamental del negocio en Europa. La **UE** ha diseñado un **marco regulatorio** cada vez más exigente que está redefiniendo los modelos operativos en sectores clave como la industria, el transporte y la energía. Las cifras son contundentes: según la **Agencia Europea de Medio Ambiente** (AEMA), más del **90% de las ciudades europeas** superan los límites de **contaminación** recomendados por la OMS, una realidad que ha llevado a Bruselas a intensificar su normativa ambiental.

Este nuevo escenario regulatorio refleja un cambio profundo en las prioridades europeas, donde la **protección de la salud pública** y la **sostenibilidad ambiental** han pasado a ser ejes estratégicos. Las empresas se enfrentan ahora al reto de integrar la gestión de la calidad del aire como parte esencial de sus sistemas de cumplimiento normativo, adaptando sus procesos a requisitos cada vez más estrictos.

Los datos de la AEMA muestran el impacto real de esta problemática: contaminantes como las **partículas finas** (PM2.5) y el **dióxido de nitrógeno** (NO2) causan anualmente cientos de miles de muertes prematuras en Europa. Estas cifras han impulsado a la **Comisión Europea** a situar la mejora de la calidad del aire en el corazón del **Pacto Verde Europeo**, el ambicioso plan que busca hacer de **Europa** el primer continente **climáticamente neutro** para **2050**.

Marco regulatorio actual: directivas clave para la normativa europea

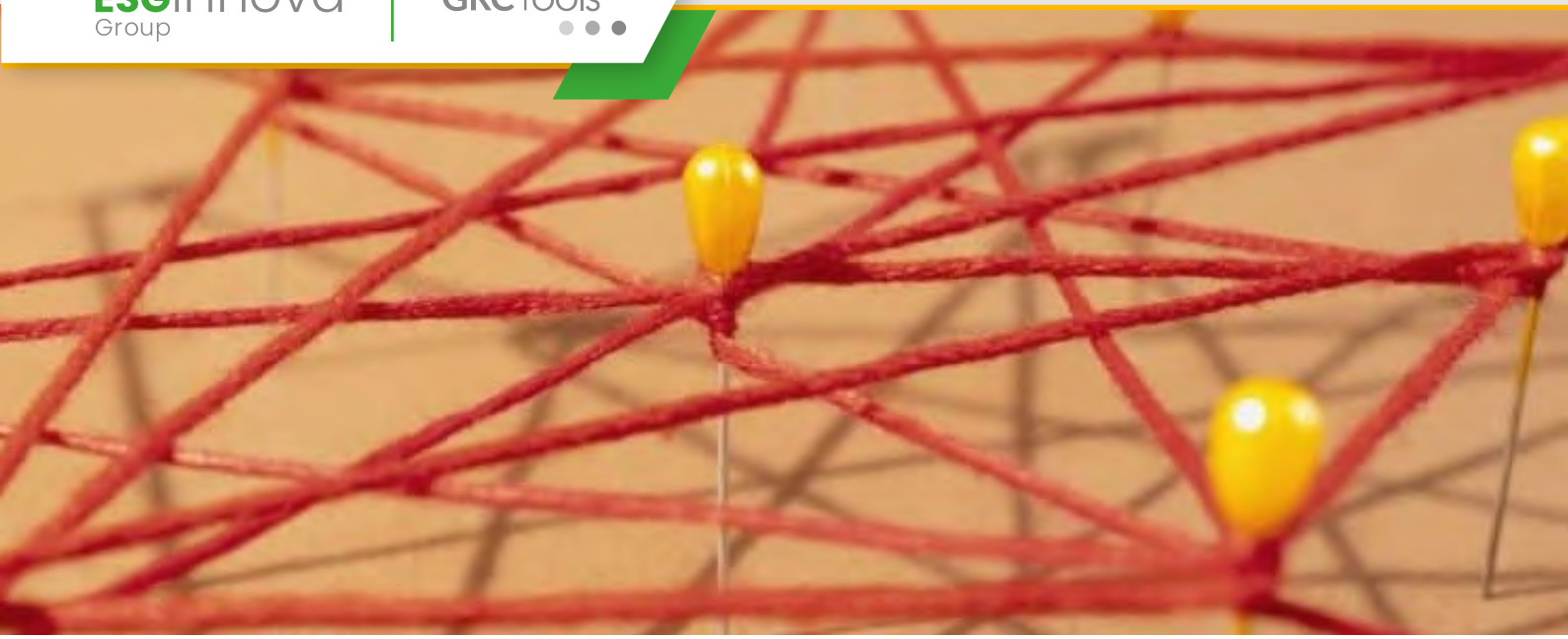
La legislación europea sobre calidad del aire se articula principalmente alrededor de dos instrumentos fundamentales. En primer lugar, la **Directiva 2008/50/CE** sobre calidad del aire ambiente, que establece valores límite para los principales contaminantes atmosféricos. Esta directiva fija umbrales específicos para **partículas en suspensión** (PM10 y PM2.5), **dióxido de nitrógeno** (NO2), **ozono troposférico** (O3), **dióxido de azufre** (SO2), **benceno** (C6H6) y otros compuestos nocivos. Los límites varían según el contaminante y el período de medición, con especial atención a los promedios anuales y las concentraciones máximas permitidas en periodos cortos.

En segundo lugar, la **Directiva (UE) 2016/2284** sobre compromisos nacionales de reducción de emisiones establece objetivos vinculantes para los estados miembros hasta 2030. Esta normativa afecta especialmente a cinco grupos de contaminantes: **óxidos de azufre** (SOx), **óxidos de nitrógeno** (NOx), **compuestos orgánicos volátiles no metánicos** (COVNM), **amoníaco** (NH3) y **partículas finas** (PM2.5). Los porcentajes de reducción varían según el país y el contaminante, con metas que oscilan entre el 30% y el 63% respecto a los niveles de 2005.

ESGinnova Group

GRCTools

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



Mapa de riesgos: tipos más importantes y algunos ejemplos

Imagina un barco navegando en aguas desconocidas. Sin un mapa que señale los peligros ocultos bajo la superficie, cada ola podría ser una amenaza imprevista. En el mundo empresarial, ese mapa existe, y se llama **mapa de riesgos**. En una era donde la incertidumbre es la norma y los desafíos evolucionan a velocidad vertiginosa, las organizaciones que no cuenten con una brújula confiable para identificar y gestionar riesgos están destinadas a naufragar.

Pero no se trata solo de evitar peligros; se trata de convertir las amenazas en oportunidades, de anticiparse a lo inesperado y de construir una cultura empresarial resiliente y preparada para el futuro. En este artículo, exploraremos los **tipos de mapas de riesgos más importantes**, ejemplos prácticos de su aplicación y cómo herramientas tecnológicas como **GRCTools** están redefiniendo la gestión de riesgos en el mundo empresarial.

¿Qué es un mapa de riesgos y por qué es esencial?

Un mapa de riesgos es una representación visual que permite a las organizaciones identificar, evaluar y priorizar los riesgos a los que están expuestas. Esta herramienta se basa en dos ejes principales: la **probabilidad de ocurrencia** y el **impacto** que tendría cada riesgo sobre los **objetivos estratégicos** de la empresa.

En el ámbito de la **Transformación Digital del Gobierno, Riesgo y Cumplimiento (GRC)**, el mapa de riesgos se convierte en un aliado indispensable para alinear la gestión de riesgos con los objetivos corporativos, garantizando el cumplimiento normativo y optimizando la toma de decisiones.

Tipos de mapas de riesgos más importantes

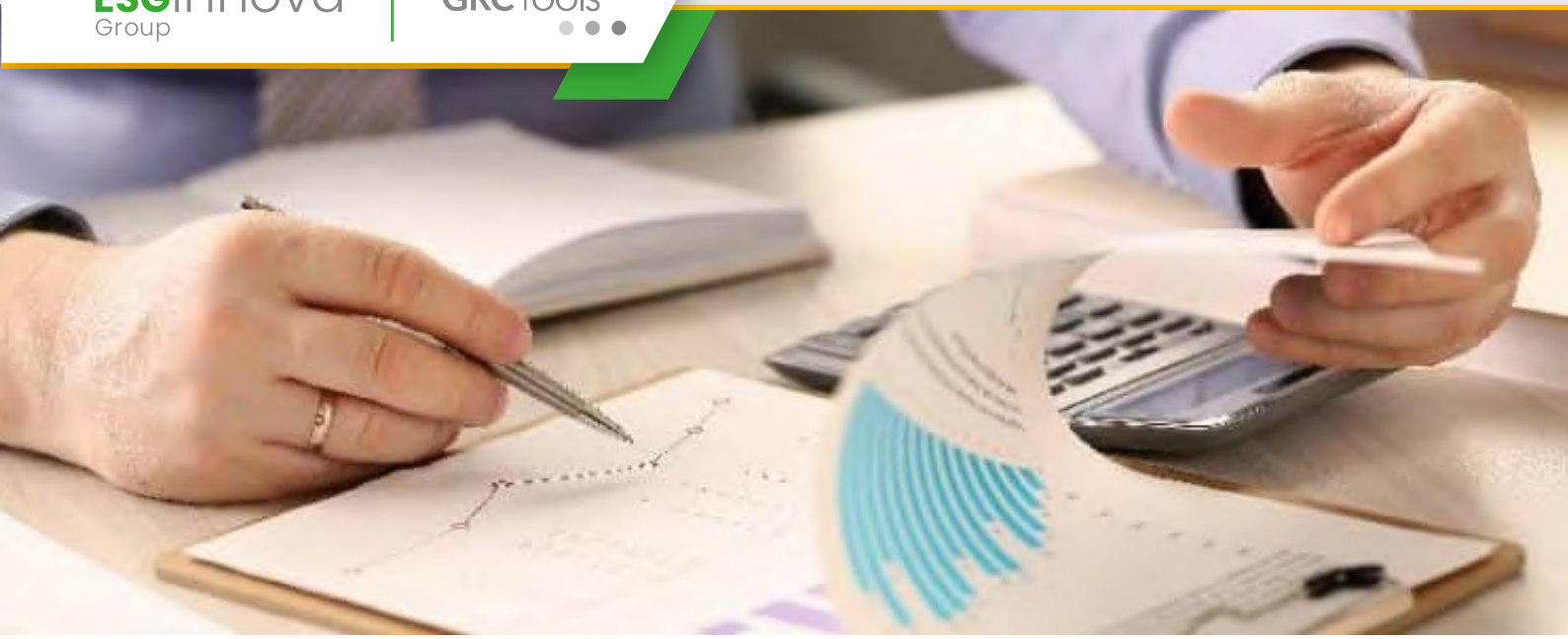
1. Mapa de riesgos por probabilidad e impacto

Este es el tipo más común y se basa en una matriz que clasifica los riesgos según su probabilidad de ocurrencia (eje X) y su impacto (eje Y). Los riesgos se ubican en cuadrantes que van desde «bajo riesgo» hasta «riesgo crítico».

Ejemplo: En una empresa de servicios financieros, un riesgo como un ciberataque podría ubicarse en el cuadrante de alta probabilidad y alto impacto, requiriendo acciones inmediatas.

2. Mapa de riesgos por categorías

Este tipo de mapa agrupa los riesgos en categorías específicas, como riesgos financieros, operativos, legales o reputacionales.



¿Qué significa control interno para una organización?

La función principal del **control interno** es garantizar la eficiencia, la transparencia y el cumplimiento normativo de las organizaciones. Pero, ¿qué significa realmente el control interno y por qué es tan crucial para el éxito empresarial?

Es necesario adentrarse en este concepto para conocer su importancia en la gestión moderna y, cómo la implementación de **herramientas tecnológicas** ayuda en la manera en que las empresas abordan este desafío.

Control interno: La columna vertebral de la gestión eficiente

El control interno es un **sistema integrado por políticas, procedimientos y prácticas** diseñadas para **proteger los activos de una organización, garantizar la precisión de la información financiera, promover la eficiencia operativa y asegurar el cumplimiento de leyes y regulaciones**.

No se trata solo de prevenir fraudes o errores, sino de crear un entorno donde los riesgos se gestionen de manera proactiva y los objetivos estratégicos se alcancen de forma consistente.

Según el marco **COSO** (*Committee of Sponsoring Organizations of the Treadway Commission*), el control interno se compone de cinco componentes interrelacionados:

01. **Entorno de control**: La base cultural y ética de la organización.

02. **Evaluación de riesgos**: Identificación y gestión de riesgos que podrían afectar los objetivos.

03. **Actividades de control**: Acciones específicas para mitigar riesgos.

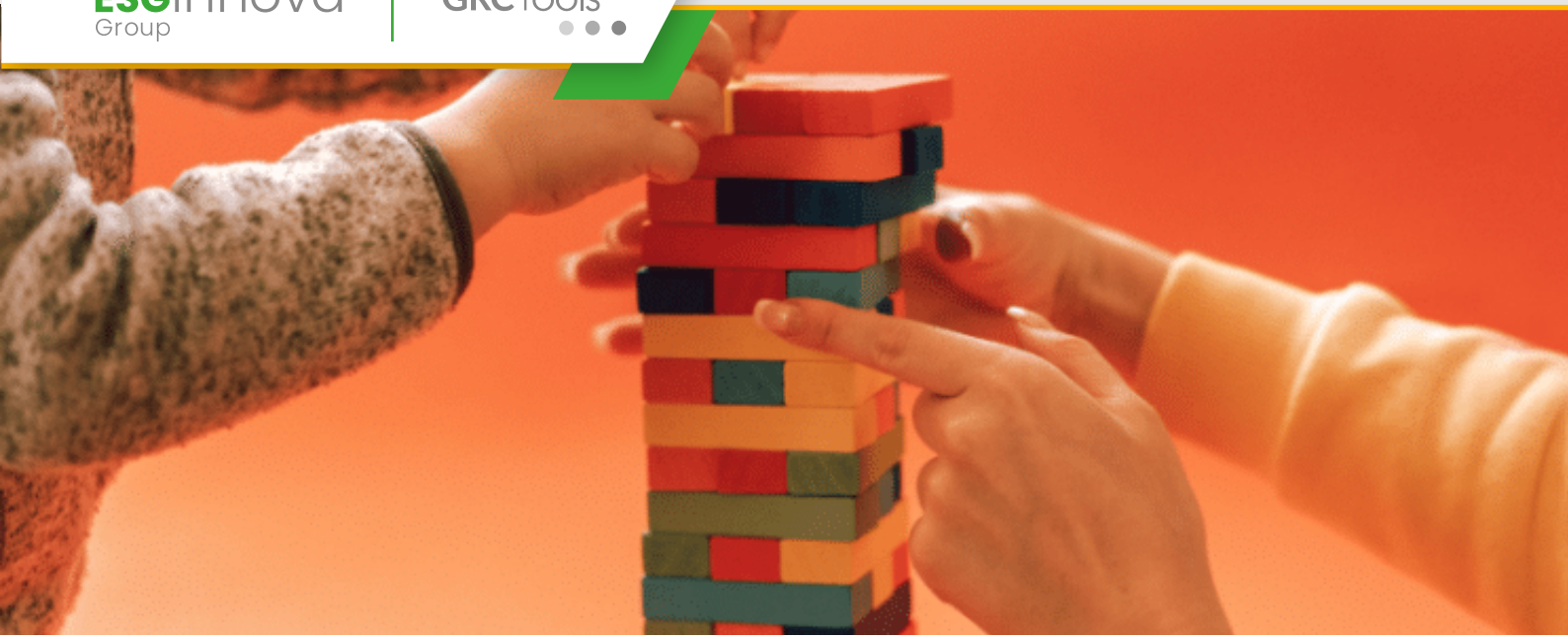
04. **Información y comunicación**: Flujo de datos relevante y oportuno.

05. **Supervisión y monitoreo**: Evaluación continua del sistema de control interno.

Estos elementos trabajan en conjunto para proporcionar una estructura robusta que permite a las organizaciones operar con **confianza** y **resiliencia**.

El control interno en el contexto de la transformación digital

La **Transformación Digital** ha revolucionado la manera en que las empresas gestionan sus operaciones, riesgos y cumplimiento.



¿Qué es Balanced Scorecard y por qué es tan importante?

En un entorno empresarial altamente competitivo, contar con herramientas que permitan **alinear la estrategia con la ejecución** es clave para el éxito organizacional. En este sentido, el **Balanced Scorecard (BSC)**, o **Cuadro de Mando Integral (CMI)**, se ha convertido en un enfoque ampliamente utilizado para **medir el desempeño y mejorar la toma de decisiones**.

El **Balanced Scorecard** permite a las empresas traducir su visión y estrategia en **objetivos medibles y alineados en cuatro perspectivas clave**: financiera, clientes, procesos internos y aprendizaje y crecimiento. Esta metodología ayuda a las organizaciones a evaluar su rendimiento de manera equilibrada y a enfocarse en los factores que realmente impulsan el **éxito a largo plazo**.

En este artículo, exploraremos en detalle qué es el **Balanced Scorecard**, sus beneficios y cómo implementarlo de manera efectiva en una empresa.

Balanced Scorecard

El **Balanced Scorecard** es un **modelo de gestión estratégica** desarrollado por **Robert Kaplan y David Norton** en la década de 1990. Su propósito es proporcionar a las organizaciones un **marco integral** para **evaluar su desempeño** más allá de los indicadores financieros tradicionales.

A diferencia de otros enfoques, el **Balanced Scorecard** permite a las empresas **medir** su **progreso** en base a cuatro perspectivas clave:

Perspectiva financiera

Evalúa el rendimiento económico de la empresa, considerando métricas como:

- **Ingresos y rentabilidad**.
- **Retorno sobre la inversión (ROI)**.
- **Flujo de caja y costos operativos**.
- **Perspectiva del cliente**

Mide la satisfacción y fidelidad de los clientes mediante indicadores como:

- **Nivel de satisfacción del cliente**.
- **Tasa de retención y adquisición de clientes**.
- **Reputación y valor de marca**.

Todo lo que debe contener una evaluacion de riesgos

Una base para lograr la sostenibilidad y trabajar por el éxito de las organizaciones es la **evaluación de riesgos**. Ya sea en el ámbito del **Gobierno, Riesgo y Cumplimiento (GRC)**, la seguridad laboral o la gestión de proyectos, una evaluación de riesgos bien estructurada va a permitir identificar y mitigar amenazas, pero también se va a encargar de optimizar procesos y tomar decisiones estratégicas con mayor confianza.

¿Sabrías detallar **todo lo que debe contener una evaluación de riesgos efectiva**? Acompáñanos durante las siguientes líneas, para conocer un enfoque especial sobre cómo las empresas pueden mejorar su gestión mediante la implementación de soluciones tecnológicas avanzadas centradas en la **Gestión Integral de Riesgos**.

¿Por qué es crucial una evaluación de riesgos en el entorno empresarial?

Las empresas enfrentan desafíos constantes: cambios regulatorios, ciberamenazas, riesgos operativos, crisis económicas y más. Una evaluación de riesgos bien diseñada ayuda a prevenir pérdidas financieras y reputacionales, al mismo tiempo que fomenta una **cultura organizacional proactiva y resiliente**.

Sin embargo, muchas organizaciones aún dependen de métodos manuales o desactualizados para gestionar riesgos, lo que puede resultar en omisiones, errores y respuestas tardías. Aquí es donde la **Transformación Digital** y las herramientas tecnológicas marcan la diferencia.

Elementos clave de una evaluación de riesgos efectiva

1. Identificación de riesgos

- **Definición del alcance**: Es fundamental delimitar el área o proceso que se va a evaluar, ya sea un departamento, un proyecto o toda la organización.
- **Fuentes de riesgo**: Identificar peligros potenciales, como fallos tecnológicos, incumplimientos normativos, riesgos financieros o de seguridad.
- **Participación de stakeholders**: Involucrar a todos los actores relevantes, desde empleados hasta directivos, para obtener una visión holística.

¿Qué certifica el ENS Esquema Nacional de Seguridad?

En el caso de la Administración Pública española y las entidades que colaboran con ella, el **ENS Esquema Nacional de Seguridad** es el marco de referencia que establece los principios y requisitos para proteger los **sistemas**, los **datos** y los **servicios digitales**. Pero, ¿qué certifica exactamente el ENS y por qué es relevante también para el sector empresarial? Si tienes dudas sobre esto, te invitamos a explorar en profundidad esta temática y cómo ciertas herramientas pueden ayudar a las empresas a alinearse con estos **estándares de seguridad**.

¿Qué es el ENS y qué certifica?

El **ENS Esquema Nacional de Seguridad**, regulado por el Real Decreto 3/2010, es un conjunto de políticas, medidas y procedimientos diseñados para garantizar la **seguridad de la información** en el ámbito público y en aquellas organizaciones privadas que interactúan con la Administración Pública. Su objetivo principal es proteger la **confidencialidad, integridad y disponibilidad** de los datos, minimizando los riesgos asociados a ciberamenazas y brechas de seguridad.

La certificación ENS Esquema Nacional de Seguridad valida que una organización cumple con los siguientes aspectos clave:

01. **Cumplimiento normativo**: La organización sigue las directrices legales y técnicas establecidas por el ENS Esquema Nacional de Seguridad.

02. **Gestión de la seguridad**: Se ha implementado un Sistema de Gestión de la Seguridad de la Información (SGSI) robusto y adaptado a los riesgos específicos de la entidad.

03. **Niveles de seguridad**: Se aplican medidas de seguridad adecuadas al nivel de protección requerido (bajo, medio o alto), en función del impacto potencial de un incidente.

04. **Auditorías y evaluaciones**: La organización se somete a auditorías periódicas para demostrar el cumplimiento continuo del ENS.

05. **Concienciación y formación**: El personal está capacitado y sensibilizado sobre las políticas de seguridad.

Para las **entidades públicas**, esta **certificación** es **obligatoria**. Sin embargo, para el sector privado, adoptar el ENS es una ventaja competitiva, que además también demuestra el compromiso con la seguridad y la protección de la información.

El ENS en el sector empresarial: Una oportunidad para mejorar

Aunque el ENS nació como un marco orientado a la Administración Pública, **su relevancia trasciende al sector empresarial**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Impacto y metodología de implantación de DORA en el sector financiero

El **Reglamento DORA** (Digital Operational Resilience Act) nace como una respuesta regulatoria clave para garantizar que las entidades financieras puedan enfrentar y superar las crecientes amenazas cibernéticas y las disrupciones tecnológicas. Es importante hablar sobre el **impacto de DORA**, su **metodología de implantación** y cómo las empresas pueden optimizar su cumplimiento mediante soluciones tecnológicas avanzadas como, por ejemplo, un **software**.

El impacto de DORA en el sector financiero: Un cambio de paradigma

DORA no es solo otra normativa; es un marco integral que redefine cómo las entidades financieras gestionan los riesgos digitales. Su impacto se extiende a múltiples dimensiones:

Resiliencia operativa como prioridad:

- DORA obliga a las entidades a adoptar un enfoque proactivo en la gestión de riesgos TIC, asegurando que puedan resistir, responder y recuperarse de incidentes como **ciberataques**, fallos técnicos o desastres naturales.

- Esto implica no solo proteger los sistemas, sino también garantizar la continuidad del negocio en escenarios críticos.

Armonización regulatoria en la UE:

- DORA establece un marco común para todos los estados miembros de la Unión Europea, eliminando la fragmentación regulatoria y facilitando la implementación de prácticas coherentes en toda la región.

Gestión rigurosa de terceros:

- Las entidades deben asegurar que sus proveedores de servicios críticos (como proveedores de **nube** o servicios de TI) cumplan con los mismos estándares de resiliencia.

- Esto implica evaluaciones exhaustivas y contratos con cláusulas específicas de cumplimiento.

Transparencia y reporting obligatorio:

- DORA exige informes detallados sobre incidentes de ciberseguridad y pruebas de resistencia, lo que aumenta la transparencia y la rendición de cuentas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué significa NERC-CIP?

La protección de infraestructuras críticas, y su impacto en la Transformación Digital del Gobierno, Riesgo y Cumplimiento, son esenciales para garantizar la estabilidad económica, la seguridad nacional y el bienestar social. En este contexto, los estándares **NERC-CIP** (North American Electric Reliability Corporation – Critical Infrastructure Protection) crean un escenario regulatorio esencial para salvaguardar la red eléctrica de América del Norte. Pero, ¿qué significa realmente NERC-CIP y por qué es relevante para la Transformación Digital del Gobierno, Riesgo y Cumplimiento (GRC)?

A lo largo de este análisis, nos adentraremos en el significado de NERC-CIP, examinaremos su relevancia en la **gestión de riesgos** y el cumplimiento regulatorio, y exploraremos cómo las empresas pueden maximizar su eficiencia en la implementación gracias a soluciones tecnológicas avanzadas como **GRCTools**, nuestra plataforma líder en software GRC.

¿Qué es NERC-CIP y por qué es crucial?

NERC-CIP es un conjunto de estándares diseñados para proteger la infraestructura crítica del **sistema eléctrico** contra amenazas físicas y cibernéticas. Su objetivo principal es garantizar la **confiabilidad** y **seguridad** de la red eléctrica, un recurso vital para el funcionamiento de la sociedad moderna.

Los estándares NERC-CIP cubren áreas clave como:

- **Identificación de activos críticos**: Determinar qué sistemas y equipos son esenciales para la operación de la red.
- **Seguridad física y cibernética**: Proteger instalaciones y sistemas contra accesos no autorizados y ciberataques.
- **Gestión de acceso**: Controlar quién y cómo se accede a los sistemas críticos.
- **Respuesta a incidentes**: Establecer protocolos para detectar, responder y recuperarse de incidentes de seguridad.

Estos estándares son un requisito regulatorio, que además ayudan a establecer una estrategia proactiva para mitigar riesgos que podrían tener consecuencias catastróficas, como **apagones masivos** o **sabotajes**.

NERC-CIP en el contexto de la Transformación Digital

La **Transformación Digital** ha revolucionado la forma en que las organizaciones gestionan sus operaciones, riesgos y cumplimiento. Sin embargo, también ha ampliado la superficie de ataque, especialmente en sectores críticos como el energético.

¿Qué establece el Real Decreto 311/2022?

El **Real Decreto 311/2022**, publicado el 3 de mayo de 2022, marca un antes y después en la regulación de la **ciberseguridad** en España. Esta normativa, que deroga y sustituye al anterior **RD 3/2010**, actualiza el **Esquema Nacional de Seguridad (ENS)** para adaptarlo a los nuevos desafíos digitales que enfrentan tanto las administraciones públicas como las empresas privadas.

En un contexto donde los **ciberataques** crecen en complejidad y frecuencia -según datos del INCIBE, España sufrió más de 100.000 incidentes críticos en 2023-, el nuevo marco regulatorio busca establecer requisitos más robustos para proteger los **sistemas de información** y los datos sensibles.

Pero más allá de ser una simple actualización normativa, el **Real Decreto 311/2022** representa una **transformación profunda** en el enfoque de la gestión de riesgos tecnológicos.

Análisis exhaustivo del Real Decreto 311/2022

Principales novedades y cambios significativos

El **Real Decreto 311/2022** introduce varias modificaciones sustanciales respecto a su predecesor:

01. **Enfoque basado en riesgo**: La normativa adopta una perspectiva más flexible, permitiendo adaptar las medidas de seguridad según el **nivel de riesgo** específico de cada organización o sistema.

02. **Perfiles de cumplimiento diferenciados**: Se establecen distintos niveles de exigencia en función de la criticidad de la información manejada y los servicios prestados.

03. **Obligatoriedad en la notificación de incidentes**: Las organizaciones deben comunicar los **incidentes graves** al **Centro Criptológico Nacional (CCN-CERT)** en plazos más estrictos.

04. **Mayor énfasis en la continuidad del negocio**: Se refuerzan los requisitos para garantizar la **resiliencia operacional** frente a ciberataques.

05. **Armonización con estándares europeos**: La normativa se alinea con el **Reglamento (UE) 2019/881** y la futura **Directiva NIS2**.

Ámbito de aplicación ampliado

Mientras que el anterior **ENS** se centraba principalmente en el sector público, el **Real Decreto 311/2022** extiende su alcance.

¿Qué es PMBOK en gestión de proyectos?

En el acelerado mundo de la transformación digital, las organizaciones enfrentan el desafío constante de alinear sus operaciones con estándares de excelencia, especialmente en áreas críticas como el Gobierno, Riesgo y Cumplimiento (GRC). En este contexto, el **PMBOK (Project Management Body of Knowledge)** emerge como un marco de referencia indispensable para la **gestión de proyectos**, ofreciendo metodologías probadas que pueden ser adaptadas a las necesidades específicas del entorno corporativo moderno.

El PMBOK: Fundamentos y evolución

Desarrollado por el **Project Management Institute (PMI)**, el PMBOK es reconocido como el estándar global en gestión de proyectos. Su última edición, la séptima, marca un cambio significativo al pasar de un enfoque basado en procesos a uno centrado en **principios y dominios de desempeño**, lo que lo hace más flexible y adaptable a metodologías ágiles e híbridas.

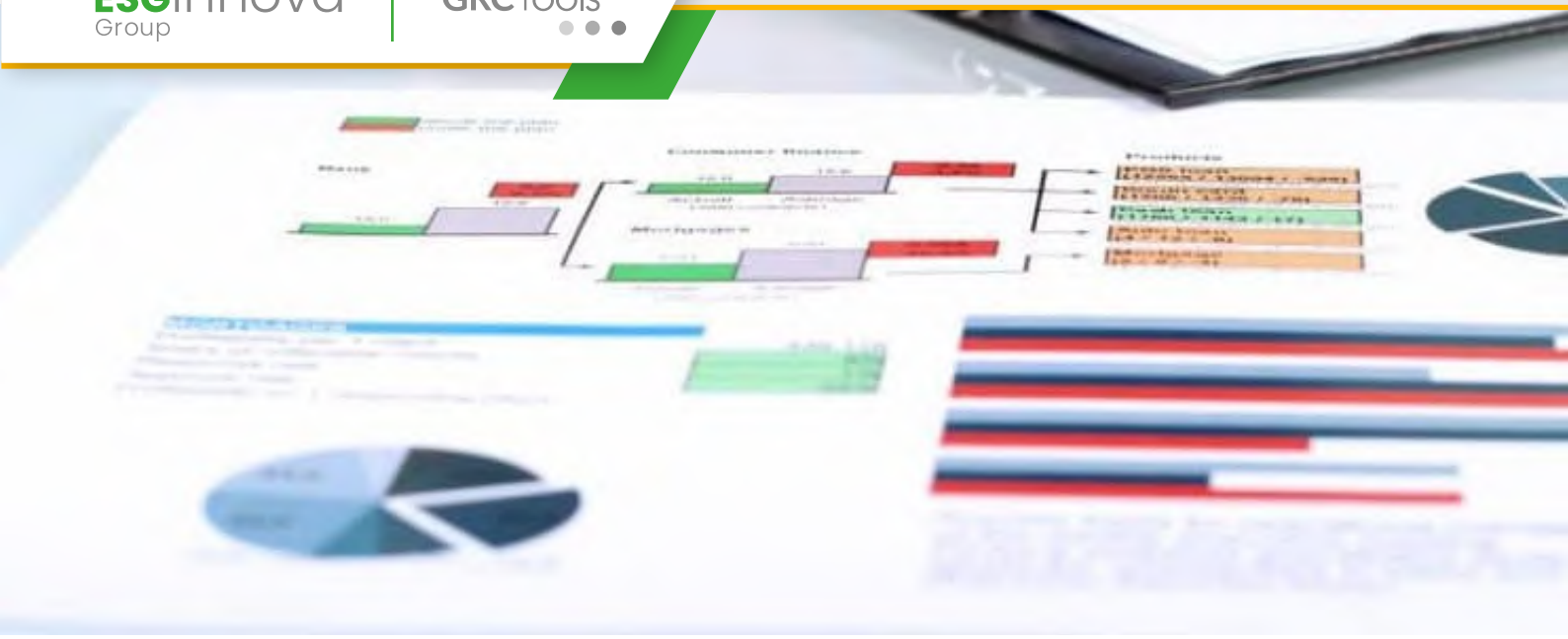
Los **12 principios del PMBOK** incluyen aspectos como la entrega de valor, la gestión proactiva de stakeholders y la adaptabilidad, todos ellos esenciales para proyectos en entornos regulados. Por otro lado, los **8 dominios de desempeño** abarcan áreas como la gestión de riesgos, recursos y cronogramas, proporcionando una estructura sólida para garantizar el éxito de las iniciativas empresariales.

La importancia del PMBOK en el ámbito corporativo

En el sector empresarial, la implementación del PMBOK no solo mejora la eficiencia en la ejecución de proyectos, sino que también fortalece los pilares del GRC. Las organizaciones que adoptan este marco experimentan beneficios tangibles en términos de **control de riesgos, cumplimiento normativo y optimización de recursos**.

Uno de los aspectos más relevantes es su contribución a la **gestión de riesgos**. Al seguir los lineamientos del PMBOK, las empresas pueden identificar y mitigar amenazas de manera temprana, reduciendo la probabilidad de incumplimientos regulatorios o fallos operativos. Además, su enfoque en la documentación y trazabilidad facilita el cumplimiento de normativas como **SOX, GDPR o ISO 31000**, lo que es especialmente valioso en industrias altamente reguladas.

Sin embargo, uno de los mayores desafíos que enfrentan las empresas es **implementar el PMBOK sin sacrificar agilidad**. Muchas organizaciones temen que la adopción de un marco tan estructurado pueda ralentizar sus procesos, especialmente en entornos donde la velocidad y la adaptabilidad son críticas.



Para qué sirve la certificación PMP

Las organizaciones enfrentan desafíos cada vez más complejos en materia de regulación, gestión de riesgos y eficiencia operativa, por tanto, la certificación **PMP (Project Management Professional)** se crea como un elemento diferenciador para profesionales y empresas que buscan optimizar su **Gestión de Proyectos** bajo un marco estructurado.

Vamos a explorar el valor estratégico de la certificación PMP en el contexto del **Gobierno Corporativo, la Gestión de Riesgos y el Cumplimiento (GRC)**, analizando cómo su implementación, junto con soluciones tecnológicas avanzadas como **GRCTools**, puede impulsar la excelencia en la ejecución de proyectos dentro de entornos altamente regulados.

El valor estratégico de la certificación PMP

La **Project Management Professional (PMP)**, otorgada por el **Project Management Institute (PMI)**, es reconocida a nivel global como un estándar de excelencia en la dirección de proyectos.

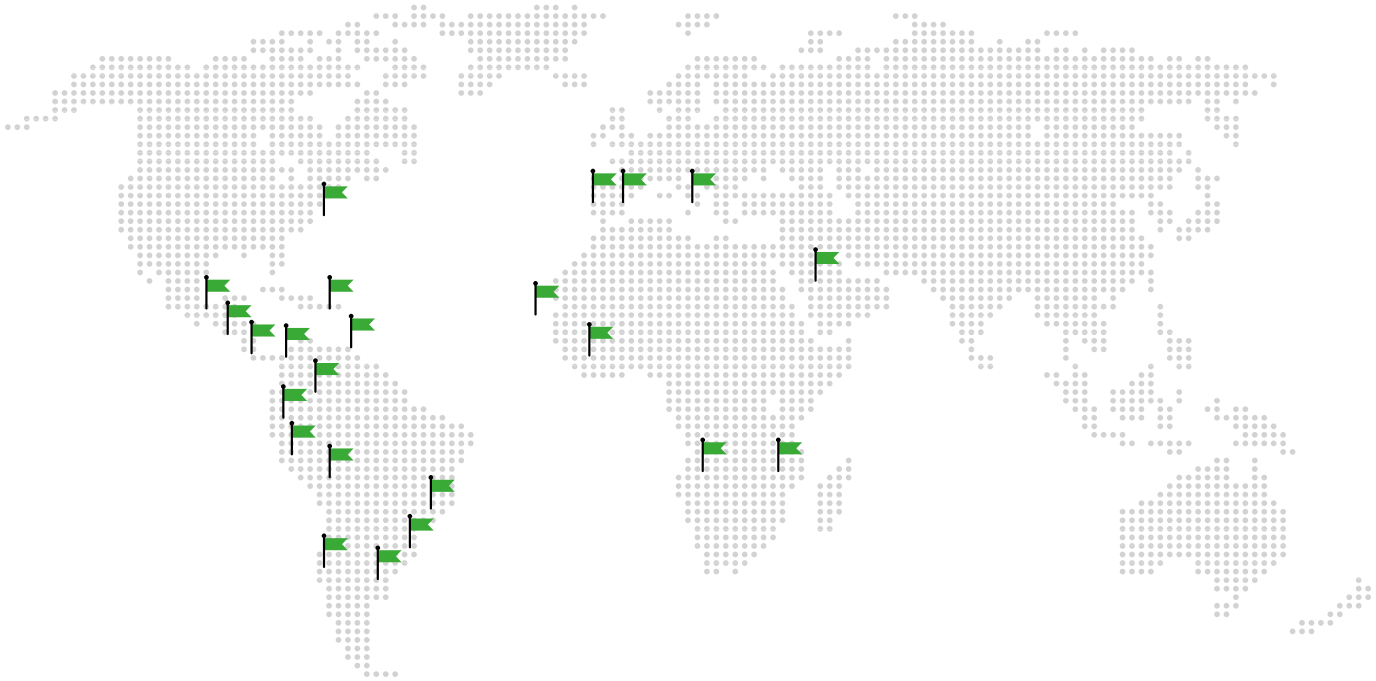
Su metodología, basada en las mejores prácticas recogidas en el **PMBOK® (Project Management Body of Knowledge)**, proporciona un enfoque sistemático para la planificación, ejecución y control de iniciativas empresariales.

Para las organizaciones que operan en sectores regulados, como el financiero, el sanitario o el energético, contar con profesionales certificados PMP garantiza que los proyectos se gestionen con un alto grado de predictibilidad, minimizando desviaciones en plazos y costos. Además, esta certificación fomenta la **alineación estratégica** entre los objetivos del proyecto y las políticas de **Gobierno Corporativo**, asegurando que cada iniciativa cumpla con los requerimientos normativos aplicables.

Uno de los aspectos más relevantes de la PMP es su enfoque en la **gestión de riesgos proactiva**. Los profesionales certificados están capacitados para identificar amenazas potenciales desde las etapas iniciales de un proyecto, implementando controles que mitiguen su impacto. Esta capacidad es especialmente valiosa en entornos donde el incumplimiento de regulaciones puede derivar en **sanciones económicas, daños reputacionales o incluso consecuencias legales**.

La certificación PMP en el contexto del gobierno corporativo y el cumplimiento normativo

El **Gobierno Corporativo** exige que las organizaciones operen con transparencia, accountability y adherencia a normativas internas y externas. En este sentido, la PMP actúa como un facilitador clave, ya que su metodología promueve la **documentación rigurosa**, la **trazabilidad de las decisiones** y la **comunicación efectiva con los stakeholders**.



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