

EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC



ENERO 2025

ESGinnova
Group

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



ACERCA DE ESG INNOVA GROUP04

NORMAS ISO9

- ✓ Requisitos legales en ISO 45001: pasos para identificarlos y darles cumplimiento.....10
- ✓ Todos los controles del Anexo A de la norma ISO 27001 explicados.....12
- ✓ El rol de ISO 42001 e ISO 27001 en sistemas de IA robustos14
- ✓ Cómo determinar objetivos de seguridad en el trabajo: ejemplos prácticos.....16
- ✓ ISO 27001: Revision por la Dirección18
- ✓ ISO 27001 y 27002: diferencias y similitudes.....20
- ✓ Normas ISO para implementar IA a considerar en el desarrollo de sistemas de inteligencia artificial22
- ✓ Como actualizar ISO 27001: Guía de transición a la nueva norma24
- ✓ ISO 53001: Sistemas de gestión de los objetivos de desarrollo sostenible de las Naciones Unidas26
- ✓ Día Internacional de la Energía Limpia 2025: El papel de la norma ISO 5000128
- ✓ ¿Cuáles son los requisitos de la futura norma ISO 53001?.....30
- ✓ Estándar de sistemas de gestión de IA: guía práctica sobre ISO/IEC 4200132
- ✓ Los beneficios de implementar un sistema de gestión medioambiental en tu negocio.....34
- ✓ ¿Qué es la norma ISO 22301 y para qué sirve?.....36
- ✓ ¿Cómo contribuye la norma ISO 53001 a los ODS?38

SEGURIDAD, SALUD Y MEDIOAMBIENTE40

- ✓ La seguridad de los contratistas y su papel en el logro de los objetivos ESG41
- ✓ Ejemplo de procedimiento de trabajo para la SST de una empresa43
- ✓ 10 tendencias en HSE a tener en cuenta en 202545
- ✓ Investigación de accidentes por el método de arbol de causas47
- ✓ Gestión de la seguridad de los contratistas: 5 errores comunes a evitar49
- ✓ ¿Qué es un diagrama de Pareto y para qué sirve?51

Índice



✓ 5 formas en las que el software de salud y seguridad puede mejorar el cumplimiento normativo	53
✓ Que es IPERC y para qué sirve	55
✓ Plataforma para la administración de contratistas: ventaja clave.....	57
✓ ¿Qué hacen los HSEQ?.....	59
✓ Inspección de seguridad, salud y medio ambiente: factores clave que se evalúan	61
✓ ¿Qué es una matriz de riesgo para la empresa?	63
✓ Software de manejo de subcontratistas: cómo superar los desafíos de implementación.....	65
✓ Quién es el contratista en una organización.....	67
✓ ¿Qué buscar en una solución de software HSE?	69
✓ Contratistas vs. proveedores. ¿Cuál es la diferencia?	71
✓ 6 elementos de la gestión de la seguridad del contratista	73
✓ Tipos y categorías de elementos de protección personal	75
GOBIERNO, RIESGO Y CUMPLIMIENTO	77
✓ ¿Qué significan las siglas BSC?	78
✓ ¿Qué es un mapa estratégico en Balanced Scorecard?	80
✓ 3 Claves para hacer un Mapa Estratégico.....	82
✓ ¿Qué dice la Ley 21663 de Chile?	84
✓ ¿Qué significan las siglas ERM?	86
✓ Cuáles son los objetivos estratégicos de una empresa y cuál es su importancia	88
✓ ¿Cómo implementar los OKR en tu proyecto empresarial?	90
✓ Importancia de la flexibilidad de la planeación operativa ante los cambios.....	92
✓ 5 ejemplos de Balanced Scorecard de una empresa	94
✓ Cómo mejorar tu gestión con un Cuadro de Mando BSC	96
✓ Guía para elaborar un Cuadro de Mando Integral Balanced Scorecard.....	98
✓ 7 ejemplos para hacer un análisis de riesgos	100
✓ Formas de alcanzar el éxito gracias a una matriz de riesgos.....	102
✓ Ley federal de protección de datos personales de México.....	104
✓ ¿Cuántos tipos de riesgos ambientales existen para una empresa?	106
✓ El camino hacia la Excelencia	108

ESG Innova Group

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

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

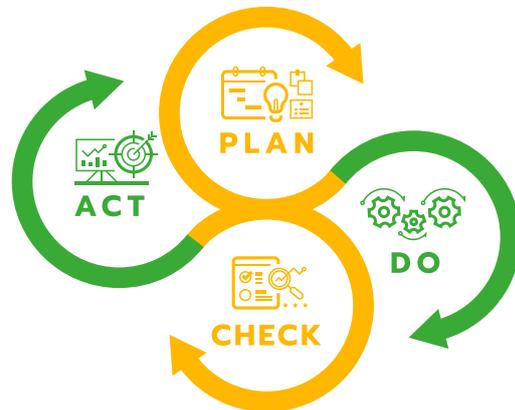
Plataforma ESG Innova

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

❖ Motor de mejora continua

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

ESGinnova
Group



❖ Plan

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

❖ Do

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

❖ Check

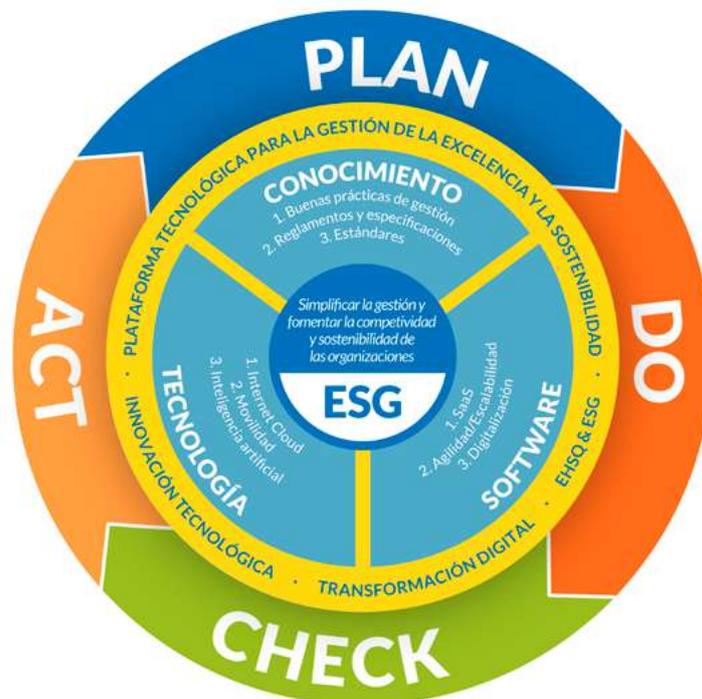
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ Act

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

Unidades de negocio

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



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

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

Unidades de negocio

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

ISOTools

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

HSETools

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

GRCTools

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

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo



Menos de tiempo de resolución de una acción correctiva



Menos de tiempo de preparación de las reuniones de gestión



Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes



Menos de intercambios de documentación física entre sedes y dptos.



Menos de costes indirectos derivados de la gestión documental



La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento



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



Más capacidad de resolución de problemas del sistema de gestión



Más de trabajadores implicados en la gestión del sistema

ISOTools



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



Requisitos legales en ISO 45001: pasos para identificarlos y darles cumplimiento

Los **requisitos legales en ISO 45001** se podrían resumir en una frase: **ISO 45001** solicita a las organizaciones cumplir con las leyes, normas, decretos, directivas o regulaciones sobre todos los temas que atañen de forma directa o indirecta a la seguridad, la salud y el bienestar de los trabajadores.

El alcance del requisito no tiene límites geográficos Esto significa que las exigencias sobre requisitos legales en ISO 45001 son válidos para una organización en cualquier país europeo, para una empresa sudamericana, en el sur de Asia, en el centro de África, en América del Norte o en la más pequeña de las islas de Oceanía. Pero los requisitos legales en ISO 45001 **también tienen alcance sobre normas supranacionales** provenientes de organizaciones como Organización Internacional del Trabajo u otra de carácter o con propósito similar.

Es importante, no obstante, **encontrar un marco que permita identificar las obligaciones de cumplimiento** en el área de seguridad y salud en el trabajo, sean estas locales, regionales, nacionales o internacionales.

Cuáles son los requisitos legales en ISO 45001

Los requisitos legales en ISO 45001 se mencionan en diferentes apartados del texto de la norma. Destacan cinco: política de seguridad, determinación de requisitos legales, definición de objetivos, evaluación de cumplimiento y revisión por parte de la Alta Dirección.

1. Requisitos legales en ISO 45001 en la política de seguridad

En cuanto a la **política SST**, la solicitud es clara e imperativa: **incluir el compromiso de la Alta Dirección con el cumplimiento** de todos los requisitos legales aplicables a nivel local, regional o internacional. Se incluyen aquellos que la empresa suscriba por voluntad propia o en acuerdo con sus empleados, con alguna asociación que los represente o con cualquier otro grupo con intereses en la seguridad y la salud de los trabajadores.

2. Determinación de los requisitos legales en ISO 45001

La cláusula 6.1.3 hace la solicitud precisa a la organización para que identifique los requisitos legales utilizando un proceso que se diseñe e implemente con ese objetivo específico. El proceso, además de identificar los requisitos legales en ISO 45001, **necesita establecer mecanismos para garantizar el cumplimiento.**



Todos los controles del Anexo A de la norma ISO 27001 explicados

La **norma ISO 27001** es el estándar internacional para la gestión de la seguridad de la información. Su objetivo principal es ayudar a las organizaciones a proteger sus datos frente a amenazas y garantizar la confidencialidad, integridad y disponibilidad de la información. Una parte clave de esta norma es el **Anexo A**, que contiene un conjunto de **controles** diseñados para abordar los riesgos de seguridad de la información. A continuación, se explican los principales controles del Anexo A de la norma ISO 27001.

Clasificación de los controles del Anexo A de la norma ISO 27001

Los **controles del Anexo A** de la norma **ISO 27001** son un conjunto de medidas diseñadas para ayudar a las organizaciones a gestionar y mitigar los riesgos relacionados con la **seguridad de la información**.

Estos controles proporcionan prácticas recomendadas que las empresas pueden implementar para garantizar la **confidencialidad, integridad y disponibilidad** de la información.

Su objetivo principal es servir como una **guía de referencia** para establecer, implementar y mantener un **Sistema de Gestión de Seguridad de la Información (SGSI)** eficaz. Los controles abordan múltiples áreas de seguridad, desde la gestión de accesos y criptografía hasta la seguridad física y la protección contra amenazas cibernéticas.

El Anexo A de la ISO 27001 (versión 2022) agrupa sus controles en **cuatro categorías principales**:

1. Controles Organizativos del Anexo A de la norma ISO 27001

Estos controles se centran en la estructura, políticas y procedimientos internos de la organización. Incluyen:

- **Políticas de seguridad de la información:** Establecen directrices claras para gestionar la seguridad.
- **Gestión de activos:** Identifican y protegen los activos de información.
- **Seguridad en los recursos humanos:** Garantizan la seguridad antes, durante y después del empleo.
- **Control de acceso:** Restringen el acceso a los datos según roles y necesidades específicas.



El rol de ISO 42001 e ISO 27001 en sistemas de IA robustos

Los **sistemas de IA** contribuyen al desarrollo de diversas **industrias tecnológicas**, pero también de empresas de todos los tamaños en sectores que van desde automoción y aeronáutica, hasta retail, logística y organizaciones financieras, pasando por el sector farmacéutico y sanitario.

Es difícil encontrar un modelo de empresa que no haga uso, en mayor o menor grado, de sistemas de IA. Por supuesto, la novedad que aún representa esta tecnología y el dinamismo y evolución que la caracterizan, **plantean retos para las empresas que necesitan establecer modelos de gobernanza y gestión sólidos.**

Las oportunidades son lo suficientemente atractivas como para **buscar opciones de gestión que garanticen la transparencia**, la privacidad de los datos y el respeto a los derechos de las personas, características esenciales en sistemas de IA robustos. Esos son los aportes que pueden hacer ISO 42001 e **ISO 27001.**

Cuáles son los objetivos de ISO 27001 e ISO 42001

ISO 27001 es el estándar con reconocimiento internacional **diseñado para gestionar los riesgos que amenazan la seguridad de la información de las organizaciones** y la privacidad de los datos de terceros que gestione la empresa. 93 controles de seguridad, distribuidos en cuatro categorías, aparecen en el **Anexo A de la norma ISO 27001**.

ISO 42001 es un reciente estándar, publicado en diciembre de 2023, para dotar de herramienta eficaces para que las organizaciones **hagan un uso seguro, responsable, ético, transparente, equitativo y respetuoso de los derechos humanos, de los sistemas de Inteligencia Artificial**. Es una norma diseñada para organizaciones que desarrollen o utilicen sistemas de IA, que también entrega controles y una guía para la implementación de esos controles en sus Anexos A y B.

El trabajo colaborativo e integrado entre ISO 42001 e ISO 27001 facilita a las organizaciones abordar los riesgos de seguridad de la información, de privacidad de datos y los inherentes al uso de IA. Se genera así confianza en los clientes y en otras partes interesadas, entre ellas los organismos reguladores.

Cuál es el alcance de los sistemas de IA

Cuando se habla de sistemas de IA se hace referencia a todos los desarrollos tecnológicos, aplicaciones, software, asistentes de voz, chatbots, algoritmos de aprendizaje o robots autónomos, entre otros. Otra cosa es el alcance de los sistemas de Inteligencia Artificial, que **se refiere a los límites físicos, virtuales o digitales que tiene la aplicación del sistema**.



Cómo determinar objetivos de seguridad en el trabajo: ejemplos prácticos

El inicio del año es momento propicio para determinar nuevos **objetivos de seguridad en el trabajo**. Lo es porque comienza un nuevo ciclo, pero también porque la evaluación de la gestión SST del año que terminó puede indicar que hay que fijar nuevas metas, eliminar algunas o pensar en una forma más efectiva de alcanzar la mejora continua, como obtener la certificación **ISO 45001**.

El objetivo será mejorar lo hecho en el año anterior. Así, **los nuevos objetivos de seguridad en el trabajo necesitan ser posibles**, útiles y surgir de una planificación cuidadosa en la que cuenta mucho la estrategia.

Cómo determinar objetivos de seguridad en el trabajo útiles

A la hora de determinar objetivos de seguridad en el trabajo útiles, el principio elemental que es preciso conocer y comprender es que **no basta con proponerlos o incluirlos en un documento o en una lista.**

Es preciso **verificar la posibilidad real de alcanzarlos y la disponibilidad de los recursos físicos, tecnológicos, humanos o financieros.** Además, hay que considerar los riesgos o problemas que pueden surgir en el camino y que tienen la posibilidad de impedir o retardar el logro del objetivo.

Existen algunas **recomendaciones básicas** de enorme utilidad para ayudar a determinar objetivos realistas, útiles y generadores de **mejora continua en seguridad y salud en el trabajo:**

1. Planificar

Los objetivos de seguridad en el trabajo no se alcanzarán por estar escritos en un documento. **Es necesario pensar en los pasos que tendrán que ejecutarse para lograrlos.** Algunos de esos objetivos pueden requerir formular objetivos menores o intermedios.

Entodosloscasos**es preciso prever los problemas, los riesgos o los contratiempos que pueden surgir,** pero también los mecanismos de supervisión, **monitoreo y medición de desempeño,** así como los indicadores que se utilizarán para medir el progreso.



ISO 27001: Revision por la Dirección

La norma **ISO 27001** es uno de los estándares más importantes en la gestión de la seguridad de la información. Dentro de sus requisitos, la **revisión por la dirección** ocupa un lugar destacado, ya que garantiza el compromiso de la alta dirección en la mejora continua del **Sistema de Gestión de Seguridad de la Información (SGSI)**. Este proceso no solo fomenta la alineación estratégica, sino que también asegura que el SGSI **sea eficaz y se adapte** a los cambios organizativos y tecnológicos.

A continuación, exploraremos los elementos esenciales de la **revisión por la dirección**, cómo llevarla a cabo de manera efectiva y qué beneficios aporta a las organizaciones.

ISO 27001: Revision por la Dirección

La **revisión por la dirección** es una actividad formal que exige la cláusula 9.3 de la norma **ISO 27001**.

Consiste en una evaluación periódica del SGSI por parte de la alta dirección para **garantizar su adecuación, eficacia y alineación** con los objetivos estratégicos de la organización.

Propósitos principales

- **Asegurar la mejora continua:** Identificar áreas de mejora en el SGSI.
- **Evaluar resultados:** Analizar los datos de auditorías internas, el cumplimiento de objetivos y las no conformidades.
- **Tomar decisiones informadas:** Proveer insumos para tomar decisiones estratégicas sobre el sistema de seguridad de la información.

Elementos Clave de la ISO 27001: Revision por la Dirección

Para cumplir con los **requisitos de la norma**, es esencial que la revisión aborde ciertos elementos.

Información de entrada

Antes de iniciar la revisión, es necesario preparar una serie de datos que servirán como base para el **análisis**. Según la norma, estos son los principales insumos:

- **Resultados de auditorías internas y externas:** Proveen evidencia sobre la conformidad del SGSI.
- **Estado de acciones correctivas y preventivas:** Analizan cómo se han tratado las no conformidades y los riesgos.



ISO 27001 y 27002: diferencias y similitudes

Las **normas ISO 27001** e **ISO 27002**, pertenecientes a la familia ISO 27000, desempeñan un papel fundamental en la gestión de la **seguridad de la información**. Aunque están interrelacionadas, cumplen funciones diferentes dentro de un sistema de gestión. En este artículo, exploraremos las **diferencias entre ISO 27001 e ISO 27002, además de sus similitudes**, y cómo las organizaciones pueden beneficiarse de su implementación utilizando herramientas tecnológicas como el **Software ISO 27001 de ISOTools**.

Diferencias entre ISO 27001 e ISO 27002

A continuación, se destacan las principales diferencias entre ISO 27001 e ISO 27002. Dos normas fundamentales para la gestión de la seguridad de la información:

- **Propósito:** Mientras que la **ISO 27001** está diseñada para establecer los requisitos necesarios para implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)**, la **ISO 27002** actúa como una **guía** práctica que proporciona directrices detalladas para la implementación de **controles específicos**.

- **Certificación:** Una diferencia clave radica en que **la ISO 27001 es certificable**, lo que permite a las organizaciones obtener una certificación oficial que valide su compromiso con la seguridad de la información. Por otro lado, **la ISO 27002 no es certificable**, ya que su objetivo principal es servir como referencia complementaria.
- **Enfoque:** La **ISO 27001** responde a la pregunta de «**qué hacer**» al establecer los controles y procesos necesarios para proteger la información, mientras que la **ISO 27002** detalla «**cómo hacerlo**» mediante la descripción de buenas prácticas y ejemplos.
- **Estructura:** La estructura de la **ISO 27001** se basa en **requisitos específicos** que deben cumplirse, mientras que la **ISO 27002** se centra en proporcionar **buenas prácticas** para implementar y gestionar los controles.

ISO 27001: El pilar del Sistema de Gestión de Seguridad de la Información (SGSI)

La **ISO 27001 es un estándar internacional** que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (**SGSI**). Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información dentro de una organización.

Aspectos clave de la ISO 27001:

01. Enfoque basado en riesgos:

- ❖ Identifica y evalúa los riesgos de seguridad de la información.



Normas ISO para implementar IA a considerar en el desarrollo de sistemas de inteligencia artificial

Las **normas ISO para implementar IA** que se consideran en el desarrollo de sistemas de **Inteligencia Artificial** cumplen diferentes roles. Unas se ocupan de los temas regulatorios, otras de los requisitos de seguridad de la información y privacidad de datos y otras de las preocupaciones éticas o de transparencia.

Algunas de las normas ISO para implementar IA se han diseñado y publicado con el propósito específico de **apoyar el desarrollo seguro de los proyectos de sistemas de Inteligencia Artificial**. Aquellas de publicación anterior a la irrupción de IA tienen objetivos y entregan requisitos que se ajustan a las necesidades de las organizaciones que tratan con aplicaciones o desarrollan sistemas de Inteligencia Artificial.

Cuáles son las normas ISO para implementar IA que se deben considerar

La razón por la que se consideran normas ISO para implementar IA es **controlar y gestionar todos los riesgos inherentes a esta tecnología**, que ha generado preocupaciones e inquietudes en las empresas, en las personas y en la sociedad en general.

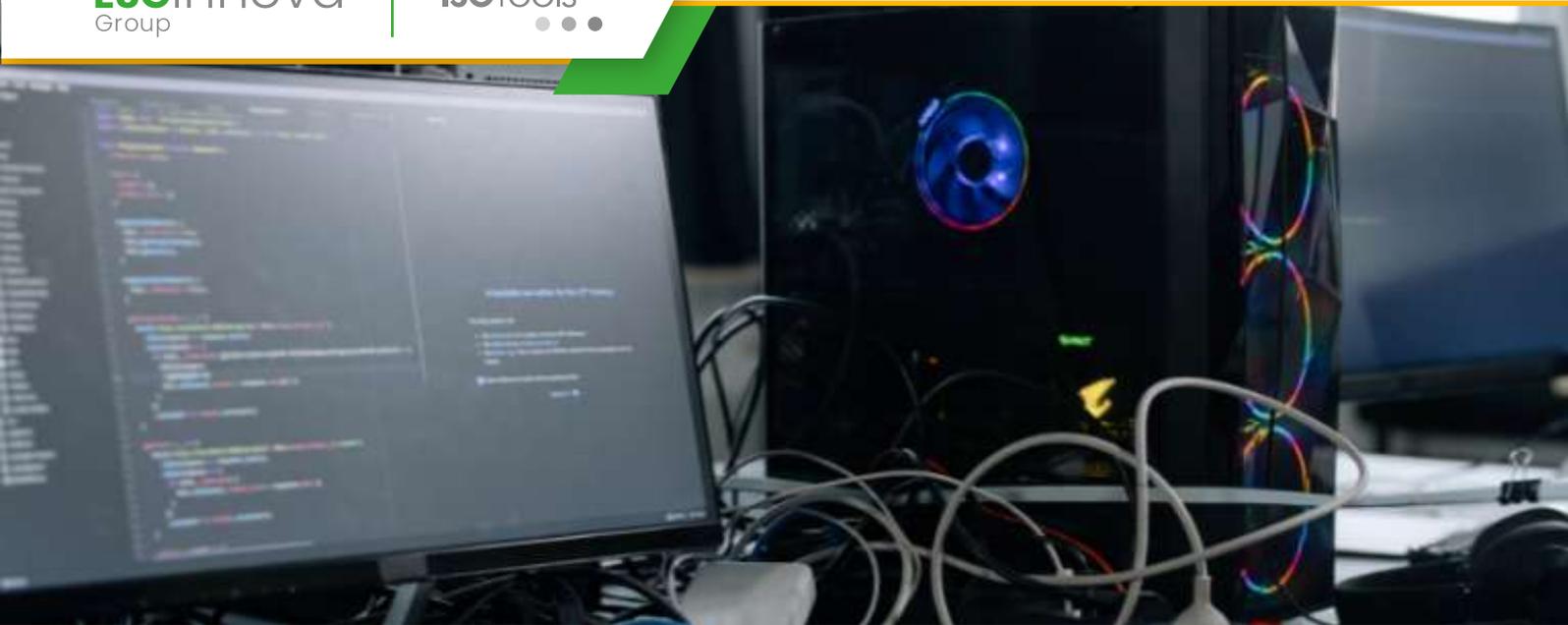
Las normas ISO para implementar IA que contribuyen al **uso seguro, transparente, legal, equitativo y ético**, son las siguientes:

1. ISO 27001 para la gestión de la seguridad de la información

ISO 27001 es el estándar internacional para gestión de riesgos de seguridad de la información. Los objetivos de la norma hacen que las organizaciones puedan tratar con seguridad el entorno en el que operan los sistemas de IA, que necesitan procesar grandes cantidades de datos confidenciales y que los destacan como objetivo de ciberataques y todo tipo de infracciones de seguridad.

La norma proporciona requisitos, orientaciones y, sobre todo, los **controles del Anexo A** para proteger la información de la organización y la de terceros.

ISO 27001 solicita a las organizaciones **gestionar, documentar, revisar, monitorear, auditar los resultados de la gestión de riesgos**, de tal forma que se garantice la mejora continua y la protección frente a amenazas externas.



Como actualizar ISO 27001: Guía de transición a la nueva norma

La **ISO 27001**, estándar internacional para la gestión de la **seguridad de la información**, ha evolucionado para mantenerse alineada con las crecientes necesidades de **protección de datos y cumplimiento normativo**. Las empresas certificadas o que buscan certificarse necesitan conocer los pasos para **actualizarse a la nueva versión de ISO 27001** de manera efectiva. Este artículo ofrece una guía detallada para gestionar esta transición y maximizar los beneficios que aporta la implementación de la norma.

Como actualizar ISO 27001

Mantener el cumplimiento y la relevancia

Con la **actualización de la norma ISO 27001**, las organizaciones deben adaptarse para:

- **Cumplir con nuevas disposiciones regulatorias:** Las regulaciones en ciberseguridad y privacidad, como el RGPD en Europa, exigen un enfoque más robusto en la gestión de riesgos.
- **Responder a las amenazas emergentes:** La digitalización ha introducido nuevos riesgos en la seguridad de la información, como el ransomware y la pérdida de datos en la nube.

Beneficios de actualizar ISO 27001

Al **adaptarse** a la nueva versión, las organizaciones pueden:

- **Fortalecer la confianza de clientes y socios:** Demostrar un compromiso actualizado con la seguridad de la información.
- **Optimizar procesos internos:** La actualización fomenta un enfoque más eficiente en la gestión de riesgos y recursos.
- **Garantizar la certificación vigente:** Cumplir con los nuevos requisitos asegura que las auditorías externas no presenten problemas.

Pasos clave para saber como actualizar ISO 27001

Analizar las diferencias entre versiones

Cambios estructurales en la norma

La nueva versión de **ISO 27001** introduce modificaciones en su estructura, como la actualización del **Anexo A** y ajustes en los **controles específicos**. Es crucial comparar las versiones anteriores y nuevas para **identificar los cambios relevantes**.



ISO 53001: Sistemas de gestión de los objetivos de desarrollo sostenible de las Naciones Unidas

Los **Objetivos de Desarrollo Sostenible** (ODS) son el corazón de la **Agenda 2030** de las **Naciones Unidas**, una hoja de ruta global que busca abordar los principales desafíos sociales, económicos y ambientales de nuestro tiempo. La **ISO 53001**, actualmente en desarrollo, está diseñada para proporcionar un marco claro y estandarizado que permita a las organizaciones integrar, gestionar y medir sus contribuciones a los ODS de manera eficaz y alineada con las mejores prácticas internacionales.

Quédate para explorar en profundidad qué es la ISO 53001, cómo beneficia a las empresas y cómo la tecnología, a través de plataformas como **ISOTools**, puede ser clave para una implementación exitosa.

¿Qué es la ISO 53001 y por qué es importante?

La **ISO 53001** es una norma que establece los requisitos para desarrollar un sistema de gestión enfocado en los **ODS**. Su objetivo principal es ayudar a las organizaciones a:

- Identificar cómo sus operaciones contribuyen a los ODS.
- Establecer metas claras y medibles relacionadas con el **desarrollo sostenible**.
- Gestionar los riesgos y oportunidades asociados a la sostenibilidad.
- Monitorear y comunicar su progreso de manera transparente.

En un mundo donde las expectativas hacia la sostenibilidad corporativa crecen día a día, la ISO 53001 se posiciona como una herramienta clave para alinear las **estrategias empresariales** con los retos globales.

¿Cómo pueden las empresas beneficiarse de la ISO 53001?

La adopción de la ISO 53001 fortalece el compromiso de una empresa con el desarrollo sostenible, a la vez que también aporta **beneficios** tangibles:

1. Mejora de la reputación corporativa

Las organizaciones que alinean sus objetivos con los ODS refuerzan su imagen ante clientes, inversores y otras partes interesadas, mostrando un **compromiso real** con el bienestar social y ambiental.



Día Internacional de la Energía Limpia 2025: El papel de la norma ISO 50001

El **Día Internacional de la Energía Limpia** es una oportunidad global para reflexionar sobre la importancia de las **fuentes de energía sostenibles y el impacto positivo** que estas tienen en el medio ambiente y la economía. En 2025, este día cobra especial relevancia debido al aumento de los compromisos internacionales para **combatir el cambio climático y alcanzar la neutralidad** de carbono. Dentro de este contexto, la **norma ISO 50001** se presenta como una herramienta clave para que las organizaciones gestionen eficazmente su consumo energético y **reduzcan su huella de carbono**.

En este artículo, exploraremos el significado del Día Internacional de la Energía Limpia, el papel de la norma ISO 50001 en la transición energética, y cómo las empresas pueden implementar estrategias sostenibles para contribuir a este esfuerzo global.

Día Internacional de la Energía Limpia

El **Día Internacional de la Energía Limpia** es una iniciativa global que busca **concienciar sobre la necesidad de adoptar prácticas sostenibles en la producción y el consumo de energía**. Este día tiene como objetivo promover el uso de fuentes de energía renovables, como la solar, eólica, hidráulica y geotérmica, y reducir la dependencia de combustibles fósiles.

En 2025, la transición hacia fuentes de energía limpia es más urgente que nunca. El cambio climático, el agotamiento de recursos naturales y la creciente demanda de energía requieren **soluciones innovadoras**. Los **beneficios** de la energía limpia incluyen:

- **Reducción de emisiones de gases de efecto invernadero:** Las fuentes renovables son esenciales para combatir el calentamiento global.
- **Diversificación de fuentes energéticas:** Minimiza la dependencia de fuentes no renovables y reduce riesgos asociados a su agotamiento.
- **Impulso a la economía verde:** Fomenta la innovación y genera empleos sostenibles.

La norma ISO 50001 en el Día Internacional de la Energía Limpia

La **norma ISO 50001** es el estándar internacional diseñado para ayudar a las organizaciones a **mejorar su desempeño energético**. Implementar esta norma no solo permite **reducir costos operativos**, sino que también contribuye a los **objetivos globales de sostenibilidad**.



¿Cuáles son los requisitos de la futura norma ISO 53001?

La gestión sostenible se ha convertido en una prioridad global, y las organizaciones que deseen mantenerse relevantes en el mercado deben alinear sus estrategias con los **Objetivos de Desarrollo Sostenible** (ODS) establecidos por la ONU. En este contexto, la futura norma **ISO 53001** promete ser una herramienta fundamental para integrar los ODS en los **sistemas de gestión empresarial**. En este artículo, exploraremos los requisitos clave de esta nueva norma y cómo su implementación puede beneficiar al sector empresarial.

Introducción a la norma ISO 53001

La ISO 53001, cuya **publicación está prevista para 2025**, establecerá un marco de referencia para que las organizaciones gestionen de manera efectiva su contribución a los ODS. Esta norma será aplicable a todo tipo de organizaciones, independientemente de su tamaño o sector, y busca fomentar un enfoque sistemático y estructurado hacia la **sostenibilidad**.

Objetivo de la norma ISO 53001

El objetivo principal de la ISO 53001 es proporcionar **directrices claras** y requisitos para que las organizaciones:

- Analicen su contexto y definan cómo sus operaciones impactan o pueden contribuir a los **ODS**.
- Identifiquen los ODS relevantes para su actividad empresarial.
- Establezcan objetivos y metas alineados con los ODS.
- Implementen acciones concretas para alcanzar estos objetivos.
- Monitoreen y evalúen los resultados obtenidos.
- Comuniquen su contribución al desarrollo sostenible a las partes interesadas.

Requisitos clave de la futura norma ISO 53001

Aunque la norma aún está en desarrollo, se espera que incluya los siguientes requisitos fundamentales:

1. Análisis del contexto de la organización

Las organizaciones deberán evaluar cómo sus operaciones, productos y servicios impactan en los **aspectos económicos, sociales y ambientales** relacionados con los ODS.



Estándar de sistemas de gestión de IA: guía práctica sobre ISO/IEC 42001

Los **sistemas de gestión de IA** cuentan con un marco normativo que facilita a las organizaciones hacer un uso responsable, ético, equitativo, legal y transparente de la Inteligencia Artificial. A la espera de otras regulaciones, los sistemas de gestión encuentran en la **norma ISO 42001** una guía confiable para asegurar el cumplimiento y el tratamiento de los riesgos asociados a la IA.

ISO 42001 entrega las herramientas necesarias para desarrollar sistemas de gestión de IA que **aseguren el uso responsable de la Inteligencia Artificial** tanto para organizaciones que la desarrollen como para aquellas otras que hagan uso de ella.

Qué es ISO 42001 para sistemas de gestión de IA

Los **órganos legislativos de diferentes países trabajan para crear un marco legal** para el uso de la IA. La Unión Europea ha tomado la delantera al publicar la **Ley de Inteligencia Artificial**,

que tiene como eje de cumplimiento el estándar ISO/IEC 42001, que es su nombre completo.

El desarrollo de sistemas de gestión de IA cambia a partir de la publicación de ISO 42001. Desde ese momento, las organizaciones **cuentan con una guía metodológica y sistemática para abordar riesgos y desafíos de IA**, pero también para aprovechar oportunidades cada vez más atractivas.

Es el enfoque metódico el que facilita el logro de los objetivos de ISO 42001. La norma permite a las organizaciones abordar riesgos como **la privacidad de datos, los derechos de las personas, las infracciones éticas** o la probabilidad de que los algoritmos preparados para aprender puedan tomar decisiones o influir en las personas para que realicen acciones que suponen autónomas.

ISO 42001 e ISO 27001

El estándar de sistemas de gestión de IA **comparte estructura de Alto Nivel** con **ISO 27001**. Los dos estándares se alinean en torno a la protección de los datos y de la información. Las dos Normas ISO entregan anexos de controles.

ISO 42001, además de la estructura de Alto Nivel, comparte otra característica reconocida en la mayoría de los estándares de reciente publicación: **la adopción del ciclo PDCA** (planear, hacer, verificar y actuar), que promueve la mejora continua.

En cuanto a los controles, ISO 42001, al igual que ISO 27001, no obliga al uso de todos los que se incluyen en el **Anexo A**. Pero sí **es preciso argumentar, en la Declaración de Aplicabilidad, las razones por las que se adoptan unos y se prescinde de otros**.



Los beneficios de implementar un sistema de gestión medioambiental en tu negocio

Implementar un **sistema de gestión medioambiental** es una decisión estratégica que tiene que ver con la competitividad, el crecimiento, el valor de la marca y la reputación de una organización. En ese marco, es importante contar con una herramienta que ayude en el proceso, como es el caso de **ISO 14001**.

Uno de los objetivos de un sistema de gestión medioambiental es **generar equilibrio entre los intereses comerciales de la organización y el logro de objetivos ambientales**. Se trata de una meta de extraordinaria relevancia en un momento de gran preocupación por el cambio climático.

Qué es un sistema de gestión medioambiental

Un sistema de gestión medioambiental es un **marco de acción creado para tratar los riesgos que pueden impactar en el medio ambiente**, el aire o las fuentes de recursos naturales como

consecuencia de las acciones que emprende la empresa con el fin de producir un bien o un servicio.

Este marco **está constituido por documentos (políticas y procedimientos), procesos, tareas y requisitos**, que interactúan para alcanzar unos objetivos. Estos, en términos generales, buscan reducir o eliminar la **huella ambiental** o cualquier afectación que cause la organización en el planeta al desarrollar sus actividades comerciales o productivas.

El objetivo general del sistema de gestión medioambiental es mejorar la relación de la empresa con el planeta. Algunos objetivos un poco más específicos incluyen **alcanzar el cumplimiento de las normas y regulaciones ambientales**, mejorar el uso de los recursos naturales, disminuir el consumo de combustibles fósiles, optimizar la gestión de residuos y sustancias contaminantes y mejorar los indicadores de impacto ambiental.

El sistema de gestión medioambiental **suele seguir el enfoque y la estructura de algún estándar con reconocimiento internacional**. El más implementado en el mundo es ISO 14001, que, entre otras ventajas, comparte la misma estructura de Alto Nivel de otras normas que son de frecuente adopción en las empresas a nivel global: **ISO 9001** o ISO 45001, entre otras. Esto facilita los procesos de implementación e integración.

Qué es ISO 14001

ISO 14001 es el estándar de gestión ambiental más utilizado en el mundo por organizaciones de todo tipo. **Incluye requisitos para que las organizaciones puedan definir su contexto, identificar riesgos, tratarlos y cumplir con cualquier obligación.**



¿Qué es la norma ISO 22301 y para qué sirve?

En un mundo donde los riesgos son cada vez más impredecibles, contar con un sistema de gestión que garantice la **continuidad del negocio** es crucial. Aquí es donde entra en juego la **norma ISO 22301**, un estándar internacional que ayuda a las organizaciones a **prepararse, responder y recuperarse de interrupciones** de manera eficiente. Este artículo ofrece una guía completa sobre esta norma, sus beneficios y cómo implementarla para fortalecer la resiliencia empresarial.

ISO 22301

La **ISO 22301** es el estándar internacional para **sistemas de gestión de la continuidad del negocio** (SGCN). Su objetivo principal es **garantizar que las organizaciones puedan operar de manera continua**, incluso frente a eventos disruptivos como desastres naturales, ciberataques, pandemias o fallos técnicos.

La norma fue desarrollada por la **Organización Internacional de Normalización (ISO)**, con la intención de proporcionar un **marco**

claro y estructurado que permita a las empresas **identificar posibles amenazas, evaluar riesgos** y establecer estrategias para **mitigar su impacto**.

El enfoque principal de la ISO 22301 es la **resiliencia organizacional**, asegurando que las operaciones críticas puedan continuar incluso en los momentos más difíciles.

Beneficios de implementar ISO 22301

Adoptar la norma ISO 22301 no solo protege a las empresas contra **interrupciones**, sino que también ofrece múltiples **ventajas competitivas**.

Mejora de la resiliencia empresarial

La ISO 22301 **ayuda** a las organizaciones a:

- **Identificar riesgos clave:** Desde desastres naturales hasta interrupciones tecnológicas.
- **Establecer planes de contingencia:** Garantizando una respuesta rápida y efectiva.
- **Asegurar la continuidad de las operaciones críticas:** Minimizar el impacto de las interrupciones en la producción, las finanzas y la reputación.



¿Cómo contribuye la norma ISO 53001 a los ODS?

La **Agenda 2030** es una hoja de ruta global que establece **17 Objetivos de Desarrollo Sostenible** (ODS) con el fin de erradicar la pobreza, proteger el planeta y garantizar la prosperidad para todos antes del año 2030. Desde su aprobación en 2015 por las **Naciones Unidas**, gobiernos, organizaciones privadas y la sociedad civil han trabajado para contribuir a estas metas. En este contexto, surge la necesidad de una herramienta estandarizada que permita a las organizaciones documentar, certificar y demostrar su contribución a los ODS.

La **futura norma ISO 53001** está actualmente en desarrollo y prevista para su publicación en **2025**. Esta se posiciona como el primer estándar internacional diseñado para establecer requisitos claros sobre cómo **las organizaciones pueden gestionar sus acciones hacia el cumplimiento de los ODS**. Este artículo analiza cómo esta norma puede ser un catalizador para la **sostenibilidad**, su impacto en el sector empresarial y el papel que juega el software de ISOTools para facilitar su implementación.

ISO 53001: Un paso hacia la certificación de la Agenda 2030

Actualmente, diversas entidades de certificación (AENOR, Bureau Veritas, entre otras) ofrecen referenciales propios para validar el compromiso de las organizaciones con la Agenda 2030. Estos modelos suelen seguir un esquema similar:

- ❖ **Estudio del contexto organizacional:** Identificación del entorno en el que opera la organización.
- ❖ **Análisis de los ODS relevantes:** Evaluación de los objetivos que mejor se alinean con la estrategia de la empresa.
- ❖ **Elaboración de un plan de sostenibilidad:** Definición de compromisos claros, objetivos medibles y acciones concretas.
- ❖ **Seguimiento y revisión:** Evaluación continua de las acciones implementadas y los resultados obtenidos.
- ❖ **Elaboración de memorias de sostenibilidad:** Comunicación de impactos y logros a las partes interesadas.

Sin embargo, estos referenciales no son estándares internacionales oficiales, lo que ha llevado a la Organización Internacional de Normalización (ISO) a trabajar en la redacción de la ISO 53001. Por tanto, esta norma busca **unificar criterios y ofrecer un marco de gestión robusto y verificable para que las organizaciones puedan demostrar su contribución efectiva a los ODS.**

HSETools



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



La seguridad de los contratistas y su papel en el logro de los objetivos ESG

La **seguridad de los contratistas** pasa por muchos exámenes, debates y estudios y también crea muchas interacciones. Pese a ello, parecería distante una relación entre la **gestión de contratistas** y la capacidad que tiene una organización para alcanzar sus objetivos ESG.

La seguridad de los contratistas es una obligación de la organización, un deber entendible con unos colaboradores estratégicos y una preocupación lógica. No tendría sentido pasar por la tarea de contratar a terceros, con los desafíos que implica la gestión, si no se espera obtener el mayor provecho de su fuerza laboral. La única forma para hacerlo es mantenerlos seguros. La pregunta que puede surgir en este escenario es qué papel desempeña la seguridad de los contratistas en el logro de los objetivos ESG de una organización. Lo explicamos a continuación.

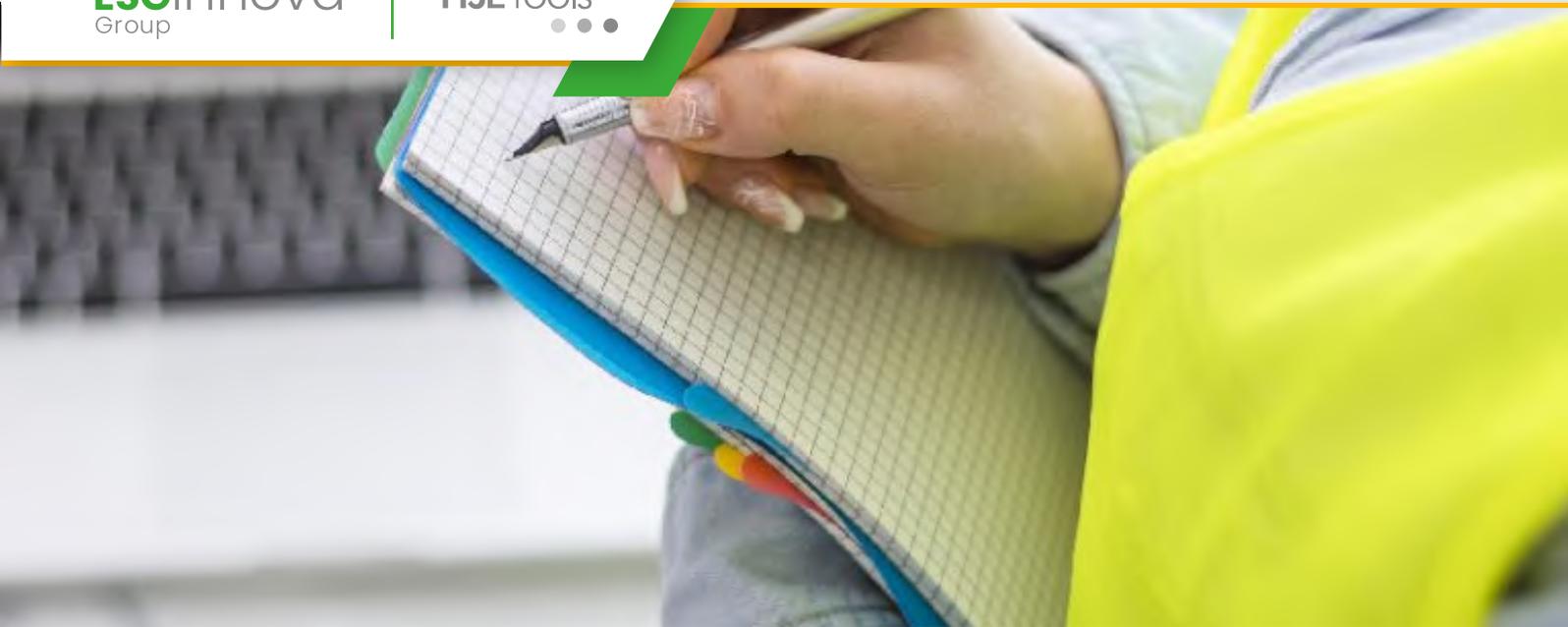
Qué son los objetivos ESG

Para entender cuál es la relación entre la seguridad de los contratistas y los objetivos ESG, es preciso entender qué son esos objetivos o criterios y cuál es su alcance. Los objetivos ESG **son las metas, obligatorias o voluntarias, que buscan alcanzar unos indicadores mínimos de mejora y productividad en tres áreas:**

- **Gestión ambiental**, que incluye el impacto sobre el planeta, la **gestión de residuos**, el uso racional de recursos naturales y energéticos, el control de emisiones de carbono y de gases de efecto invernadero o la capacidad para reutilizar materiales.
- **Aspectos sociales**, incluyendo el buen trato y la justa remuneración de los empleados, pero también las condiciones de seguridad y salud de trabajadores directos de la organización, así como de sus contratistas.
- **Gobernanza**, que habla de las acciones que emprende la organización para desarrollar su operación y que necesitan ubicarse dentro de un marco de transparencia, equidad, legalidad y ética.

Cómo se relacionan los objetivos ESG con la seguridad de los contratistas

La relación entre la seguridad de los contratistas y los aspectos sociales y de gobernanza, ejes de la gestión ESG, es fácil de explicar. El vínculo con la **gestión ambiental**, que parecería un tanto más difuso, no lo es tanto en la práctica.



Ejemplo de procedimiento de trabajo para la SST de una empresa

La **Seguridad y Salud en el Trabajo (SST)** es un pilar fundamental para garantizar ambientes laborales seguros, prevenir accidentes y proteger el bienestar de los empleados. Una herramienta clave para lograr estos objetivos es la creación e implementación de **procedimientos de trabajo** específicos para cada tarea. Este artículo explora cómo diseñar un procedimiento eficaz para la SST en una empresa y cómo optimizar su aplicación mediante herramientas digitales como el **Software de Gestión de Riesgos de HSETools**.

Ejemplo de procedimiento de trabajo para la SST

Un **procedimiento de trabajo seguro** es un documento detallado que establece las instrucciones paso a paso para realizar una tarea de manera eficiente y segura. Su propósito principal es **identificar y controlar los riesgos laborales**, proporcionando directrices claras sobre el uso de equipos, el empleo de medidas preventivas y la respuesta ante emergencias.

Además, estos procedimientos actúan como una guía formal que asegura la **estandarización de prácticas laborales**, reduciendo errores y garantizando la consistencia en la ejecución de tareas críticas. Son especialmente útiles en sectores de alto riesgo, como la construcción, la industria química y la manufactura, donde una desviación en el proceso puede tener consecuencias graves.

El desarrollo e implementación de procedimientos de trabajo para la SST también contribuyen al **cumplimiento normativo**, ayudando a las empresas a alinearse con las leyes y regulaciones laborales vigentes. Esto evita sanciones legales, y además también refuerza la imagen corporativa como organización responsable y comprometida con la seguridad.

Por último, estos procedimientos facilitan la **capacitación y formación continua** de los trabajadores, proporcionando una base documentada para la enseñanza de nuevas prácticas y la incorporación de nuevos empleados. Al establecer estándares claros, las empresas pueden crear una **cultura organizacional** orientada a la seguridad y la **mejora continua**.

Elementos esenciales de un procedimiento de SST

Para que un procedimiento sea eficaz, debe contener los siguientes elementos:

- **Objetivo:** Define el propósito del procedimiento y su alcance. Por ejemplo, garantizar la seguridad durante el mantenimiento de equipos industriales.
- **Alcance:** Especifica las actividades, áreas o personas involucradas en el procedimiento.



10 tendencias en HSE a tener en cuenta en 2025

El inicio de un nuevo año lleva a los profesionales en el área a hacer un repaso por las **tendencias en HSE** que definirán el trabajo en el campo de la **seguridad y la salud de los trabajadores** y el logro de objetivos ambientales.

Las cuestiones que se definirán como tendencias en HSE en 2025 son el **resultado de la constante evolución** en esta área tan importante para las organizaciones. La tecnología, el marco regulatorio, los comportamientos de las personas e incluso el clima y el impacto del calentamiento global son factores que definen tendencias. Los especialistas en el área necesitan obtener una comprensión clara del panorama sobre el que trabajarán en 2025. Las tendencias en HSE ayudarán a **crear hojas de ruta seguras para una gestión de riesgos eficaz**.

Tendencias en HSE que predominarán en 2025

Si se piensa de una forma racional y crítica, **en una organización todo tiene alguna relación directa o indirecta con la gestión**

HSE. El contexto de la empresa, interno o externo, es mucho más relevante para la **gestión de la seguridad y salud en el trabajo** y para los esfuerzos que se hacen para minimizar el impacto ambiental. La permeabilidad que experimenta el área HSE en relación con cualquier elemento externo es lo que explica que las siguientes sean calificadas como las **10 tendencias en HSE más relevantes en 2025**:

1. Incremento de la dependencia de los contratistas

Las organizaciones modernas encuentran en la fuerza laboral externa una interesante oportunidad. **Los contratistas se convierten en piezas clave para la ejecución de proyectos específicos**, fuera de las instalaciones de la empresa y con un atractivo valor agregado: es posible elegir el perfil del trabajador ideal para realizar trabajos en altura, en confinamiento, en condiciones climáticas extremas y, sobre todo, en cualquier lugar del mundo. La ductilidad y la facilidad para configurar un tipo de trabajador ideal para una tarea específica **no exime a la organización de sus obligaciones** con respecto a la **seguridad de los contratistas**, su salud, el cumplimiento normativo, los acuerdos económicos y el impacto ambiental del trabajo que realizan.

Por eso, una de las tendencias en HSE más destacadas es la **implementación de un software de gestión de contratistas** que **aborde todas las etapas del ciclo de vida de un contrato**, desde la selección hasta el cierre, pasando por la contratación, la ejecución, el control documental y la garantía de cumplimiento de los compromisos de ambas partes.



Investigación de accidentes por el método de árbol de causas

La **investigación de accidentes laborales** es una actividad esencial dentro de cualquier organización comprometida con la seguridad y salud de sus trabajadores. Uno de los métodos más efectivos para este análisis es el **método del Árbol de Causas**, una herramienta que permite desentrañar las relaciones entre los diversos factores que contribuyen a un incidente.

Acompáñanos en la exploración de esta metodología y cómo su implementación puede beneficiar al sector empresarial. Además, destacaremos la importancia de usar un software como **HSETools** para optimizar este proceso y lograr resultados más eficientes.

¿Qué es el método del Árbol de Causas?

El **método del Árbol de Causas** es una técnica de investigación de accidentes que permite representar, de forma gráfica y estructurada, las relaciones entre los eventos, condiciones y decisiones que llevaron

a un accidente laboral. Este enfoque parte del principio de que los accidentes no son provocados por una única causa, sino por una cadena de factores que interactúan entre sí.

Mediante la construcción de un árbol invertido, el accidente (evento principal) se coloca en la base, mientras que las causas se desglosan y ramifican hacia arriba. Esto permite analizar las **causas inmediatas** (acciones u omisiones directamente relacionadas con el accidente), y también las **causas básicas** (deficiencias organizativas, falta de formación o fallos en los sistemas de gestión).

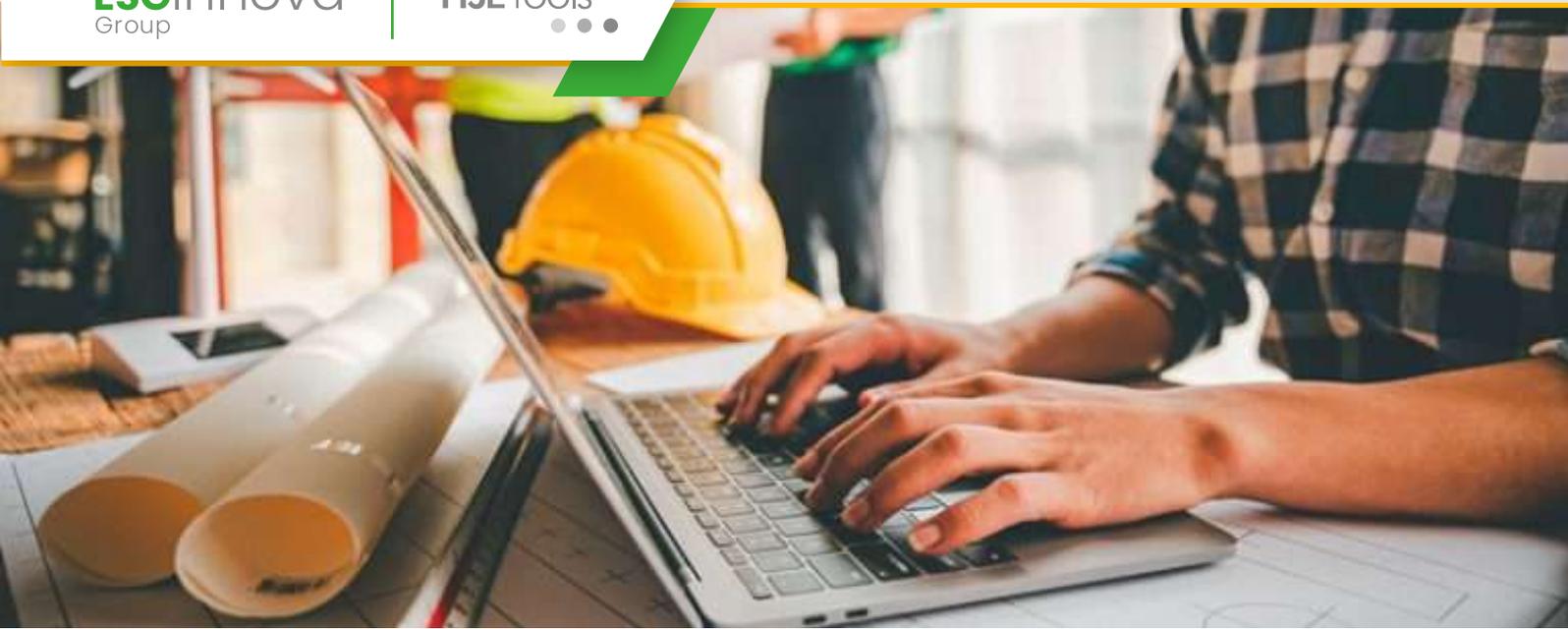
Pasos para aplicar el método del Arbol de Causas

1. Recopilación de información:

- Entrevistar a testigos y trabajadores involucrados.
- Analizar documentos relacionados, como reportes de inspección o registros de mantenimiento.
- Examinar el lugar del accidente y recopilar evidencia visual (fotos o videos).

2. Definir el evento principal:

- Identificar y describir claramente el accidente que se desea investigar. Por ejemplo, «caída desde una escalera durante una inspección de rutina».



Gestión de la seguridad de los contratistas: 5 errores comunes a evitar

La **gestión de la seguridad de los contratistas** suele ser fuente de preocupaciones para los profesionales especializados en esta área. En parte, es una cuestión relacionada con una percepción errónea de que la **seguridad de terceros** no es responsabilidad de la organización en el mismo grado que la de los empleados.

Otro desafío a los que se enfrenta la gestión de la seguridad de los contratistas es la falsa sensación de capacidad que pueden transmitir. Cuando una organización elige ejecutar un proyecto con terceros, busca aprovechar el conocimiento y la experiencia que tal vez no encuentra dentro de la organización. Se considera que ellos **están mejor capacitados y dotados para asumir ciertos riesgos**. La suma de estos supuestos lleva a **cometer errores en la gestión de la seguridad de los contratistas que pueden resultar costosos**, comprometer el éxito de un proyecto y, lo que es peor, trascender hasta impactar en la seguridad de los empleados.

Por qué es importante la gestión de la seguridad de los contratistas

La gestión de la seguridad de los contratistas permite implementar procedimientos y protocolos que se han diseñado pensando en las características únicas de este modelo de contratación. La gestión de contratistas **identifica, elimina o trata riesgos y amenazas para terceros**, pero también los que se derivan de la interacción que estos pueden tener con los empleados de la empresa o con otros terceros eventuales. La gestión de los contratistas **crea, inculca y promueve cultura de seguridad y salud en el trabajo**, que impacta de forma positiva en los mismos contratistas, pero también a los empleados de la organización:

- **Garantiza el cumplimiento** normativo y regulatorio.
- **Protege a la organización de litigios judiciales**, multas, sanciones u otra clase de penalizaciones.
- **Permite seleccionar contratistas más capaces**, eficientes y preparados para acometer los proyectos.
- **Mejora la imagen de la empresa como empleadora**, especialmente entre los contratistas que tienen una demanda de sus servicios constante gracias a su capacidad y la excelencia en su trabajo.

Errores comunes en la gestión de la seguridad de los contratistas

Pese a la importancia del trabajo, todavía muchas empresas recaen en los mismos errores.



¿Qué es un diagrama de Pareto y para qué sirve?

El **diagrama de Pareto** es una herramienta fundamental en la **gestión empresarial y la mejora de procesos**. Su simplicidad y efectividad han hecho que sea ampliamente utilizado en diversas industrias, especialmente en áreas relacionadas con la **calidad, la seguridad y la salud en el trabajo** (HSE).

Este artículo explora en detalle qué es un diagrama de Pareto, cómo se construye y cuáles son sus aplicaciones más relevantes en el entorno laboral.

Diagrama de Pareto

El **diagrama de Pareto** es una **representación gráfica** basada en el **principio 80/20**, formulado por el economista italiano Vilfredo Pareto. Este principio establece que, en muchos casos, el **80% de las consecuencias provienen del 20% de las causas**. El diagrama ayuda a **identificar y priorizar los problemas** más significativos para maximizar los esfuerzos en su solución.

Características principales

- **Orden descendente:** Muestra las causas o problemas de mayor a menor impacto.
- **Análisis dual:** Combina un gráfico de barras y una línea acumulativa para mostrar el porcentaje total.
- **Prioridad:** Facilita la toma de decisiones al destacar las áreas más críticas que requieren atención inmediata.

¿Cómo se construye un diagrama de Pareto?

Crear un **diagrama de Pareto** es un proceso sencillo que consta de varios pasos. A continuación, se presenta una **guía paso a paso**:

1. Identificar y recopilar datos

El primer paso es determinar qué **aspectos se analizarán**, como incidentes, defectos, o riesgos. Luego, se **recopilan los datos necesarios** para entender la magnitud de cada problema.

2. Clasificar las causas

Organiza las causas en categorías que representen los **diferentes problemas o factores** que deseas **analizar**. Por ejemplo, en un contexto de **seguridad laboral**, las categorías pueden incluir «caídas», «contacto con maquinaria» o «exposición a sustancias químicas».



5 formas en las que el software de salud y seguridad puede mejorar el cumplimiento normativo

Un **software de salud y seguridad** es una herramienta tecnológica que demuestra efectividad en el propósito de **mitigar o eliminar riesgos**, particularmente en industrias en las que las amenazas son constantes y tienen un alto poder lesivo.

Además de agilizar procesos, crear canales interactivos de comunicación y automatizar las tareas de la gestión, un software de salud y seguridad ofrece un atractivo beneficio adicional: **garantiza el cumplimiento normativo**.

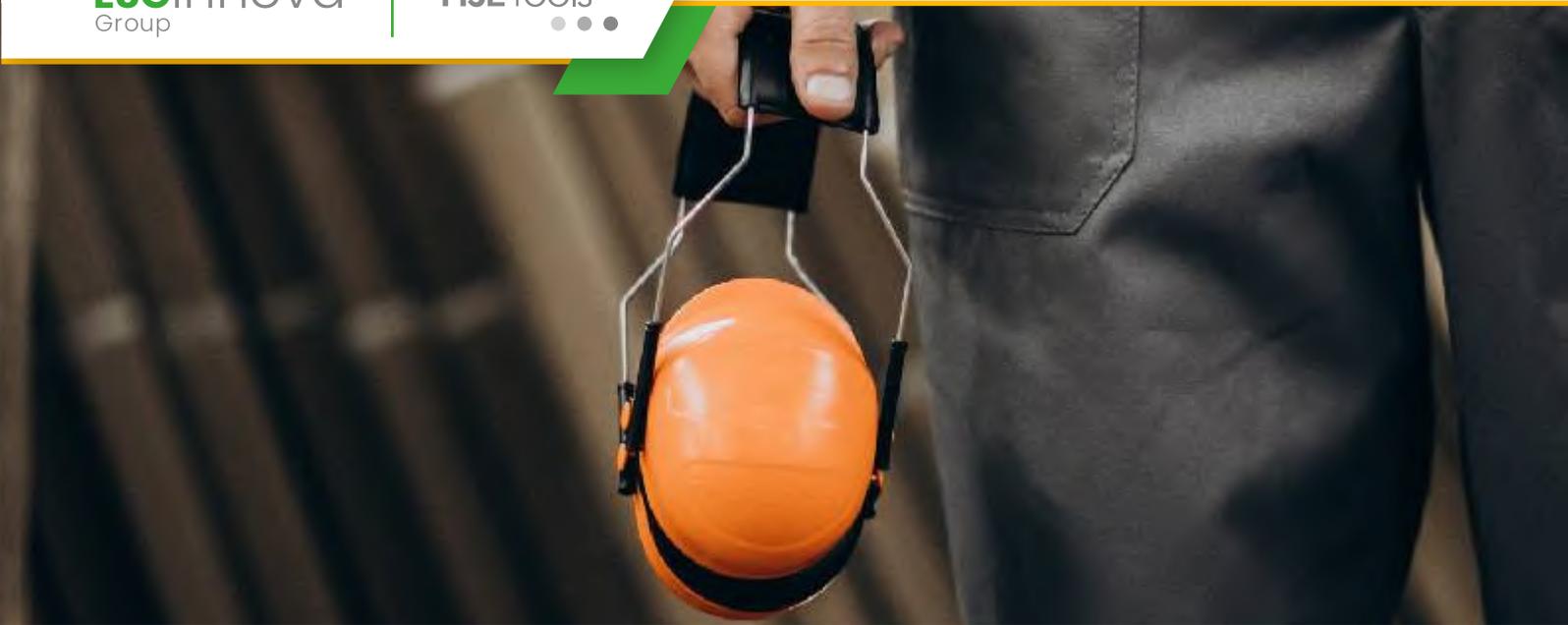
Cómo asegura el cumplimiento normativo un software de salud y seguridad en el trabajo

Cumplir con las normas internas y externas es, sin duda, la mejor manera de garantizar la seguridad de las personas en una

organización. En ese escenario, el software de salud y seguridad en el trabajo **es una solución que aborda los problemas desde un enfoque integral**. La solución puede contribuir a reducir el número de accidentes y asegurar que la **notificación de incidentes laborales** o casi accidentes se realice con facilidad. Para ello, aprovecha al máximo la **utilidad que suponen los reportes en el campo de la prevención** y del diseño de estrategias para eliminar riesgos antes de que afecten a los trabajadores. El enfoque ahora es hacia la forma en que el software de salud y seguridad en el trabajo aborda el cumplimiento normativo. Se detallan a continuación **cinco funcionalidades que demuestran efectividad en el propósito de asegurar el cumplimiento normativo**:

1. Gestión de incidentes

La resistencia o negligencia en la notificación de incidentes es una realidad. Las razones, en muchos casos, están relacionadas con la **complejidad que implica cumplir los formalismos del informe**, la ineficacia que los empleados perciben en la tarea o la posibilidad de ser responsabilizados o de que se culpe a un compañero. El software de salud y seguridad en el trabajo permite a los empleados **informar sobre cualquier hecho anómalo, desde el mismo lugar y momento** en que sucede. Además, es posible hacerlo a través de cualquier dispositivo móvil, adjuntando información en los formatos más dúctiles y que representan menos esfuerzo para el trabajador: voz, vídeo, imágenes, etc. Los canales de comunicación que entrega un software de salud y seguridad en el trabajo son de doble vía. Significa que el trabajador recibe información sobre el proceso de **investigación de accidentes** o incidentes que inicia el software de forma automática.



Que es IPERC y para qué sirve

En el mundo de la **Seguridad y Salud en el Trabajo (SST)**, uno de los conceptos clave es el **IPERC**, que corresponde a la **Identificación de Peligros, Evaluación y Control de Riesgos**. Este proceso constituye una herramienta indispensable para prevenir accidentes y enfermedades laborales, además de ser un componente esencial en la estrategia de sostenibilidad y cumplimiento normativo de cualquier organización.

Para entender bien este concepto vamos a desarrollar qué es el IPERC, cómo se aplica y cómo un software especializado, como el que ofrece **HSETools**, puede marcar la diferencia en el sector empresarial.

¿Qué es el IPERC?

El **IPERC** es un proceso sistemático que permite identificar peligros en los lugares de trabajo, evaluar los riesgos asociados y establecer medidas de control para reducirlos o eliminarlos. Este enfoque integral busca garantizar un entorno laboral seguro, saludable y productivo, alineado con las normativas locales e internacionales de SST.

Los tres pilares del IPERC

- 01. Identificación de peligros:** Consiste en reconocer todas aquellas situaciones, condiciones o actividades que puedan causar daño. Por ejemplo, una maquinaria sin protección adecuada o la exposición a sustancias tóxicas.
- 02. Evaluación de riesgos:** Una vez identificados los peligros, se analizan los riesgos considerando dos factores clave: la probabilidad de que ocurra un incidente y la severidad de sus consecuencias.
- 03. Control de riesgos:** En esta etapa se implementan medidas correctivas o preventivas, como controles administrativos, tecnológicos, de ingeniería o el uso de equipos de protección personal (EPP).

¿Para qué sirve el IPERC?

El objetivo principal del IPERC es la **prevención de accidentes y enfermedades ocupacionales**, promoviendo un entorno laboral más seguro. Sin embargo, sus beneficios van mucho más allá de la seguridad física:

- ❖ **Cumplimiento normativo:** Ayuda a las empresas a cumplir con regulaciones nacionales e internacionales, como la **ISO 45001**.
- ❖ **Optimización de procesos:** Identifica riesgos operativos que pueden causar interrupciones o pérdidas.
- ❖ **Reducción de costos:** Al prevenir accidentes y enfermedades, se reducen los costos asociados a indemnizaciones, etc.



Plataforma para la administración de contratistas: ventaja clave

Una **gestión de contratistas** eficaz es un desafío para muchas organizaciones que apoyan parte de sus operaciones en terceros. Garantizar el cumplimiento, la seguridad en el trabajo y la productividad son grandes objetivos y, para alcanzarlos, una **plataforma para la administración de contratistas** es herramienta esencial.

La transición al uso de la plataforma para la administración de contratistas implica innumerables beneficios. También conlleva algunos desafíos, como reticencias de los empleados o la infraestructura tecnológica necesaria. Son objeciones, en cualquier caso, fáciles de superar.

Cómo funciona la gestión sin una plataforma para la administración de contratistas

La gestión de la **seguridad de los contratistas** tradicional **suele desarrollarse con base en documentos en papel que nunca son**

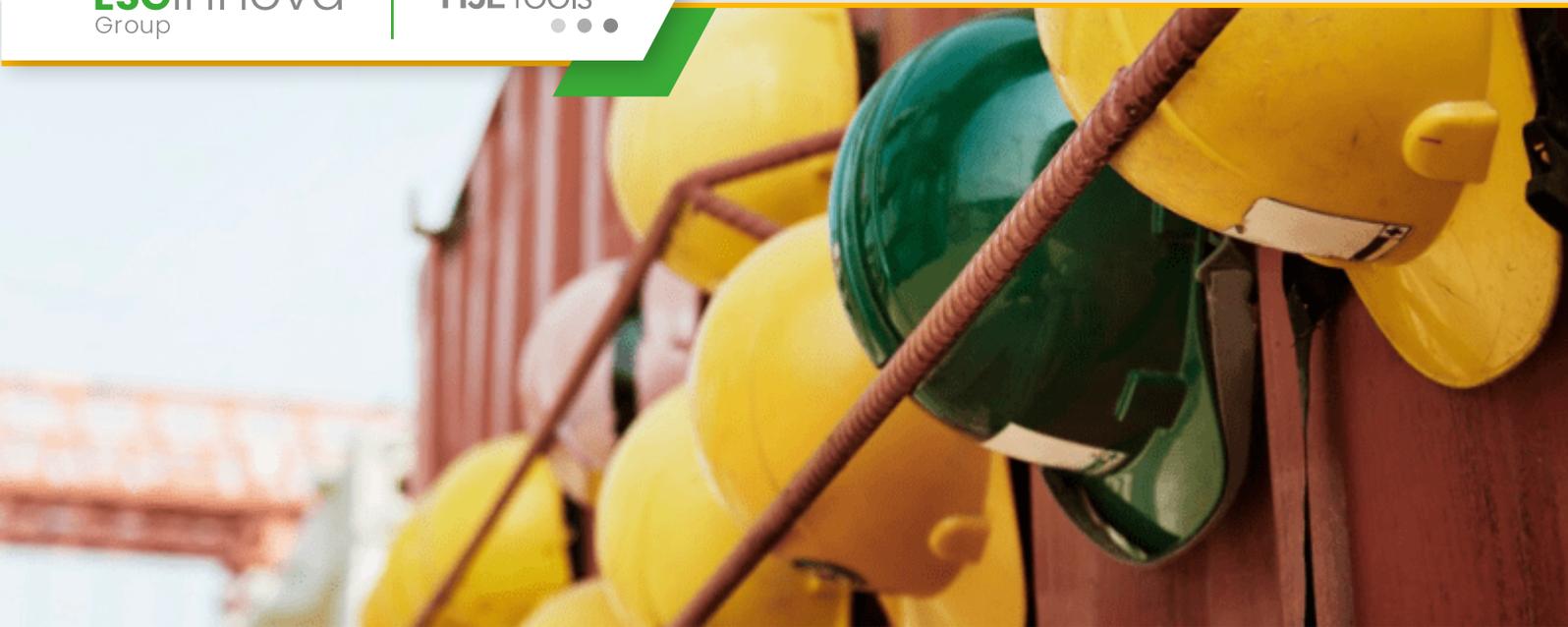
digitalizados y provienen de fuentes que no siempre mantienen comunicación entre sí: el propio contratista, el área de Recursos Humanos de la organización, alguna institución que certifica un proceso de capacitación, etc. Todo ello tiene consecuencias.

Dificultades en la gestión documental

En un escenario con un número elevado de contratistas, **uno de los mayores retos es administrar un volumen tan alto de papeles**. Se requiere almacenarlos de forma segura, garantizar la accesibilidad inmediata y no encontrar problemas para entregar un informe o garantizar que los contratistas cumplen con todos los requisitos normativos internos de la organización o regulatorios externos.

Ausencia de control

El **control de documentación de contratistas** es solo una parte del problema. Sin una plataforma para la administración de contratistas es muy complicado tener una visión constante de su labor. **Comprobar el cumplimiento normativo, regulatorio y contractual se convierte en un gran reto**. Por supuesto, **no es posible imaginar un canal de comunicación directo entre el contratista y la organización**. Deficiencias en la ejecución del trabajo, incumplimiento de las normas de seguridad, inconformidad con el cumplimiento desde las dos partes o malentendidos son consecuencias de lo que se puede calificar como una mala gestión de contratistas. El incremento de accidentes e incidentes es previsible, así como sanciones generadas por el desarrollo de trabajos sin supervisión. **Habrán costes financieros y menoscabo de la reputación de la organización**. Es el panorama en el que se desenvuelve la gestión que prescinde del uso de una plataforma para la administración de contratistas.



¿Qué hacen los HSEQ?

En un mundo empresarial cada vez más enfocado en la **sostenibilidad y el cumplimiento de normativas**, los roles relacionados con **HSEQ** (Health, Safety, Environment, and Quality) son fundamentales. Estas siglas representan las disciplinas que garantizan la **seguridad, la salud, la calidad** y el respeto por el **medio ambiente** en las operaciones de una organización.

En este artículo, exploraremos las funciones de los **profesionales de HSEQ**, su impacto en las empresas y cómo el uso de herramientas especializadas, como el **Software de HSETools**, puede optimizar su labor.

HSEQ

El término **HSEQ** engloba cuatro áreas clave:

- **Health (Salud):** Fomentar el bienestar físico y mental de los empleados.
- **Safety (Seguridad):** Minimizar riesgos y prevenir accidentes laborales.

- **Environment (Medio Ambiente):** Gestionar el impacto ambiental de las actividades empresariales.
- **Quality (Calidad):** Garantizar que los productos y servicios cumplan con los estándares establecidos.

Estas áreas trabajan de forma conjunta para asegurar un **enfoque integral** que beneficie tanto a las organizaciones como a sus empleados y el entorno que los rodea.

¿Qué hacen los profesionales de HSEQ?

Los **profesionales de HSEQ** tienen un papel estratégico dentro de las organizaciones. Algunas de sus **funciones** clave incluyen:

Identificación y gestión de riesgos

- **Evaluar riesgos laborales:** Analizan los entornos de trabajo para identificar posibles peligros.
- **Diseñar medidas preventivas:** Proponen estrategias para mitigar riesgos en salud, seguridad, medio ambiente y calidad.

Desarrollo de políticas y procedimientos

- **Elaborar políticas de HSEQ:** Diseñan documentos que establecen directrices claras para cumplir con estándares normativos y regulatorios.
- **Actualizar procedimientos internos:** Garantizan que los protocolos estén alineados con las mejores prácticas y normativas actuales.



Inspección de seguridad, salud y medio ambiente: factores clave que se evalúan

La **inspección de seguridad, salud y medio ambiente** es la actividad más relevante para la **gestión HSE** por el resultado inmediato que entrega. La inspección es una evaluación que busca verificar que la organización adopta protocolos y estándares de seguridad, prevención, cumplimiento e higiene, entre otros aspectos. La inspección de seguridad, salud y medio ambiente **se desarrolla sobre el terreno, con base en observación de procesos reales y espacios de trabajo verdaderos**. Aunque se solicitan documentos, estos pasan a un segundo plano cuando se trata de comprobar condiciones de trabajo reales. La inspección de seguridad, salud y medio ambiente puede ser practicada por un tercero, por un organismo regulador o por la misma organización. En cualquier caso, es una actividad que permite obtener **una visión directa y con alto grado de certidumbre sobre lo que está pasando y sobre el avance de la gestión HSE**.

Quiénes realizan la inspección de seguridad, salud y medio ambiente

Es **un profesional con competencias y conocimientos específicos** quien debe hacerse cargo de la inspección de seguridad, salud y medio ambiente. Es importante, por otra parte, entender que existen **diferencias entre auditoría e inspección de seguridad y salud**. Las inspecciones distan mucho de ser auditorías. Si bien estas últimas tienen gran importancia para la gestión, la inspección, por su carácter inmediato, cercano al espacio de trabajo y porque **tiene entre sus funciones comprobar el cumplimiento regulatorio y normativo**, requiere un profesional con un perfil único. El trabajo del inspector de seguridad, salud y medio ambiente busca un objetivo esencial: proteger al trabajador, en primera instancia, y luego, no con menor empeño, a la comunidad. La inspección de seguridad, salud y medio ambiente puede ser realizada por un organismo estatal regulador. De hecho, suele ser así. Pero **también puede responder a la solicitud de un tercero o practicarla la misma organización**. En cualquiera de los casos, los resultados serán útiles para la gestión, siempre que se evalúen los factores clave.

Factores clave que se evalúan en la inspección de seguridad, salud y medio ambiente

Los factores clave para evaluar en una inspección de seguridad, salud y medio ambiente **varían de acuerdo con la industria, el marco regulatorio al que esté sometida la empresa** y los acuerdos a los que hayan llegado con grupos de interés o con la comunidad.



¿Qué es una matriz de riesgo para la empresa?

Enfrentarse a riesgos es inevitable para cualquier organización o empresa. Sin embargo, la clave del éxito no radica en evitarlos por completo, sino en gestionarlos de manera eficiente. Para ello se utilizan diferentes herramientas como, por ejemplo, la **matriz de riesgo**, una solución fundamental para cualquier organización que busque minimizar amenazas y maximizar oportunidades. A través de las siguientes líneas trataremos qué es una matriz de riesgo, cómo puede beneficiar a las empresas y por qué implementar un Software de **Gestión de Riesgos**, como el que ofrece **HSETools**, es una decisión estratégica.

¿Qué es una matriz de riesgo?

Una **matriz de riesgo** es un diagrama visual que permite clasificar y priorizar los riesgos de una organización en función de dos factores clave:

01. Probabilidad: La posibilidad de que un riesgo se materialice.

02. Impacto: Las consecuencias que dicho riesgo tendría si llegara a ocurrir.

Se representa generalmente como una cuadrícula donde los riesgos se distribuyen en categorías como **bajo, medio** o **alto** según estas dos dimensiones. Este enfoque permite identificar con claridad cuáles son los riesgos más críticos y cómo abordarlos.

Por ejemplo, un riesgo con alta probabilidad y alto impacto (como una falla grave en la maquinaria de producción) ocupará un lugar prioritario en la matriz, requiriendo acción inmediata.

Importancia de la matriz de riesgo en el ámbito empresarial

En un entorno empresarial cada vez más competitivo y complejo, las empresas se enfrentan a un sinfín de incertidumbres: fluctuaciones del mercado, cambios regulatorios, amenazas a la seguridad y problemas ambientales, entre otros. La gestión adecuada de estos riesgos es esencial para garantizar la **sostenibilidad** y el crecimiento de la organización.

Beneficios de implementar una matriz de riesgo

- **Priorización eficiente:** Permite centrar los recursos en los riesgos que realmente importan.
- **Reducción de costos:** Al anticiparse a problemas potenciales, las empresas pueden evitar gastos imprevistos.
- **Mejor toma de decisiones:** Ofrece información clara y estructurada para fundamentar estrategias.



Software de manejo de subcontratistas: cómo superar los desafíos de implementación

La implementación de un **software de manejo de subcontratistas**, como otras tareas propias de la **gestión de trabajadores externos** y eventuales, supone retos que debe afrontar cualquier organización que haga uso de esta modalidad de contratación. Los desafíos que implica la implementación de un software de manejo de subcontratistas, no obstante, no tienen por qué ser causa de retraso o abandono del proyecto. Al contrario. Los riesgos de seguridad, la probabilidad de incumplimiento normativo y regulatorio o la imposibilidad de verificar el cumplimiento de las normas de seguridad o de los acuerdos contractuales de contratistas y subcontratistas, **justifican trabajar en la forma de superar los desafíos inherentes al uso de la tecnología.**

Cómo superar los desafíos de implementación de un software de manejo de subcontratistas

Un software de manejo de subcontratistas entrega grandes ventajas: **elimina procesos complicados y obsoletos, digitaliza documentos**, ofrece canales de comunicación fluidos e interactivos, estimula la productividad, disminuye costes de operación y minimiza el error humano. A esos **beneficios de la implementación de un software de gestión de contratistas** todavía hay que sumar **la automatización, la emisión de alertas y notificaciones y la creación de bases de datos de excepcional utilidad para la empresa**. Lo que resta entonces es trabajar en asumir los desafíos inherentes a la implementación del software.

1. Coste del software

Todos los proyectos de inversión requieren aprobación de la Alta Dirección. Por supuesto, **el coste es un factor determinante** para obtener el aval. La implementación del software de manejo de subcontratistas, a primera vista, supondría pagar una licencia, comprar dispositivos, servidores y periféricos, costes de capacitación y, probablemente, pagar valores adicionales cuando se alcance un número determinado de usuarios.

¿Cómo superarlo?

Contratar una solución SaaS, un software basado en la nube, elimina esos costes. Por supuesto, será preciso pagar un valor por el servicio, pero es una inversión que tiene un retorno garantizado: elimina **riesgos de cumplimiento del contratista**, evita sanciones y multas, disminuye el consumo de horas de trabajo de empleados, aumenta la productividad, etc.



Quién es el contratista en una organización

En el mundo laboral, el término **contratista** juega un papel fundamental, especialmente en sectores como la construcción, la minería, la manufactura y la logística. A menudo, el éxito de un proyecto depende de la **correcta gestión de estos actores externos**. Pero, ¿quién es exactamente el contratista y cuál es su función en una organización? En este artículo, desglosaremos el concepto, exploraremos sus **responsabilidades** y analizaremos cómo gestionar su desempeño de manera **eficiente**, alineados con las **normativas de HSE (Health, Safety and Environment)**.

Contratista

El **contratista** es una **persona o empresa externa contratada por una organización para realizar tareas específicas dentro de un proyecto**. A diferencia de los empleados directos, los contratistas trabajan bajo un **contrato independiente** y son responsables de ejecutar actividades en áreas que requieren una **experiencia especializada** o **recursos adicionales**.

Existen diferentes **categorías de contratistas** según su rol y ámbito de trabajo:

- **Contratistas generales:** Son responsables de la ejecución general de un proyecto, gestionando a su vez subcontratistas y proveedores.
- **Subcontratistas:** Trabajan bajo la supervisión del contratista general, realizando tareas específicas como instalaciones eléctricas, plomería o pintura.
- **Contratistas independientes:** Profesionales que trabajan de manera autónoma, sin equipo o personal a cargo.

Responsabilidades de un contratista en una organización

La relación entre una organización y un contratista está basada en el **cumplimiento de objetivos específicos**. Algunas de las principales responsabilidades de un contratista incluyen:

Cumplimiento de normativas de seguridad y salud

En el ámbito de **HSE**, los contratistas tienen la obligación de **adherirse a las políticas y estándares de seguridad** de la organización. Esto implica:

- ❖ Utilizar equipos de protección personal (EPP).
- ❖ Capacitarse en los procedimientos de seguridad específicos del proyecto.
- ❖ Reportar riesgos o incidentes inmediatamente.



¿Qué buscar en una solución de software HSE?

El tránsito de papel a hojas de cálculo fue un paso importante en la historia de la **gestión HSE**. Ahora muchas empresas se enfrentan a la transición hacia una **solución de software HSE**. Las ventajas que ofrece son muchas: eliminación del error humano, flujos de trabajo automáticos, alertas y notificaciones son solo algunas de ellas.

La solución de software HSE **es una herramienta diseñada para fomentar el trabajo en equipo y la interacción en tiempo real**, así como para entregar opciones que permiten monitoreo y vigilancia online desde cualquier tipo de dispositivo. A la hora de elegir una solución de software HSE es fundamental **tener en cuenta algunos factores importantes**. De ellos depende que la organización encuentre el aliado tecnológico que realmente necesita y que satisfaga todas sus necesidades.

Qué buscar en una solución de software HSE

Las razones por las que una organización busca una solución de software HSE no siempre coinciden. **El tamaño y sector de**

la organización tienen mucho que ver con los criterios de elección. También es relevante el grado de transformación digital que haya alcanzado la empresa. En cualquiera de los casos, los siguientes cinco factores son determinantes en el proceso de selección:

1. Gestión de incidentes

La inmediatez y la facilidad con la que un trabajador o un contratista puedan **interactuar con los responsables de HSE para reportar un incidente** es esencial. Permitirá iniciar un proceso de **investigación de accidentes**, incidentes y resolución del problema. Poder adjuntar información en el formato que mayor facilidad le entregue en el momento en que ocurre el evento es una funcionalidad gran valor en una solución de software HSE.

2. Creación de flujos de trabajo automáticos

Automatización es la palabra clave en este tipo de soluciones. Reportado el incidente, la rapidez con la que se produce el informe puede estar condicionada por un periodo considerable de tiempo, en tanto se conforma un equipo de trabajo, se asignan tareas y se entiende la verdadera complejidad del problema. Si **la solución puede crear el flujo de trabajo de forma automática y asignar funciones**, el proceso no perderá el ritmo inicial, para beneficio de la seguridad de todos los trabajadores.

3. Emitir alertas y notificaciones

Una solución de software HSE puede crear el flujo de trabajo y conformar el equipo que se encargará de la investigación. Es muy importante que la solución pueda notificar a las personas indicadas sobre estos y otros hechos relevantes de la gestión.



Contratistas vs. proveedores. ¿Cuál es la diferencia?

En el mundo empresarial, **los contratistas y los proveedores desempeñan roles fundamentales**, pero muchas veces se tiende a confundir sus funciones. Esta confusión puede generar inconvenientes en la gestión de operaciones, seguridad y cumplimiento normativo. En este artículo, te explicaremos de manera didáctica cuál es la diferencia entre contratistas y proveedores, por qué es importante diferenciarlos y cómo la implementación de un **Software de Gestión de Contratistas** como HSETools puede ser la clave para una administración eficiente y segura.

¿Qué son los contratistas?

Un contratista es una persona o empresa que **ofrece servicios especializados a una organización** durante un tiempo determinado. Los contratistas suelen involucrarse directamente en las operaciones del negocio, ya sea realizando tareas específicas o gestionando proyectos completos.

Características clave de un contratista:

- ❖ Proporcionan **servicios técnicos o especializados**.
- ❖ Pueden tener empleados a su cargo para cumplir con el servicio.
- ❖ Su trabajo puede implicar **riesgos en seguridad y salud** si se realiza en las instalaciones del cliente.
- ❖ Su relación contractual es compleja y exige el cumplimiento de normativas y estándares de calidad.

Ejemplo: Una empresa de construcción contrata a una firma externa para la instalación de sistemas eléctricos en un edificio.

La importancia de diferenciarlos en el sector empresarial

Para las empresas, es crucial distinguir entre contratistas y proveedores, ya que **cada grupo requiere una gestión distinta** en términos de seguridad, documentación, cumplimiento legal y evaluación de desempeño.

Beneficios de una buena gestión:

- **Mejora de la seguridad laboral:** Al gestionar adecuadamente a los contratistas, se reducen los riesgos asociados a trabajos peligrosos.
- **Cumplimiento normativo:** Mantener registros claros de contratistas y proveedores ayuda a cumplir con normativas legales y de calidad.



6 elementos de la gestión de la seguridad del contratista

Las empresas que acumulan experiencia con trabajadores externos saben cuántos detalles y aristas tiene la **gestión de la seguridad del contratista**. Construir espacios de trabajo seguros es una tarea que requiere planificación, programación, presupuesto, conocimiento y tecnología.

Los encargados de la seguridad y salud en el trabajo son los responsables directos de la gestión de la seguridad del contratista. Pese a ello, **es una responsabilidad compartida** en la que también tienen obligaciones la Alta Dirección, el director del área de Recursos Humanos y, por supuesto, el director del proyecto o del área que hace uso de terceros. Fijar los objetivos correctos e implementar un sistema de gestión de la seguridad del contratista es esencial para **proteger a la organización de posibles eventualidades**. Por supuesto, redundará en el bienestar y la tranquilidad de los mismos contratistas, pero también de los empleados directos y de visitantes eventuales.

Elementos esenciales de la gestión de la seguridad del contratista

Una adecuada gestión de la seguridad del contratista **minimiza el riesgo de multas, sanciones o cierres de operaciones**. Con ello, además, se protege la reputación de la organización. A cambio, se requiere de recursos, tiempo y algunos elementos esenciales.

1. Políticas y procedimientos

Políticas y procedimientos son la guía para alcanzar cualquier objetivo. En términos muy básicos, **las políticas expresan lo que se desea lograr** y los procedimientos la forma detallada cómo se espera que se haga. La política de seguridad de los contratistas afirma el compromiso de la Alta Dirección con su bienestar y la decisión de asignar los recursos necesarios para ello. **Los procedimientos se dividen en operativos y de prevención y seguridad**. Los primeros recopilan las instrucciones y formalidades técnicas sobre cómo desarrollar las tareas para las que se contrató al trabajador. Los segundos desglosan los protocolos de seguridad que debe seguir el contratista, algunos de ellos relacionados con el uso de **equipos de protección en el lugar de trabajo**, uso adecuado de herramientas o capacitaciones sobre cómo proceder en una emergencia.

2. Capacitación y formación

Un sistema de gestión de la seguridad del contratista, bien planificado y dotado con los recursos suficientes, puede fracasar a causa de brechas de conocimiento y formación. Los empleados necesitan formación sobre su propia seguridad y la de sus compañeros. Una opción para cerrar las brechas de conocimiento es **incluir en el perfil del contratista ideal las acreditaciones que demuestran que cuenta con la formación necesaria**.



Tipos y categorías de elementos de protección personal

En cualquier entorno laboral, la seguridad de los trabajadores es una prioridad. Los **elementos de protección personal (EPP)** juegan un papel **fundamental** en la **prevención de accidentes y enfermedades laborales**. Estos equipos están diseñados para **proteger al personal frente a riesgos** específicos asociados a sus actividades diarias. En este artículo, exploraremos los tipos, categorías y usos de los EPP, así como su importancia en la gestión de la seguridad laboral.

Elementos de protección personal

Los **elementos de protección personal (EPP)** son **equipos o dispositivos que los trabajadores deben utilizar para protegerse de los riesgos** presentes en su lugar de trabajo. Estos riesgos pueden ser de naturaleza física, química, biológica o incluso psicosocial.

Según las **normativas de seguridad**, como la **ISO 45001**, el uso adecuado de EPP es una **medida complementaria** a otras estrategias de control de riesgos, como la ingeniería o la capacitación.

Importancia de los elementos de protección personal

El uso de EPP no solo es una **obligación legal** en la mayoría de los países, sino también una herramienta clave para **garantizar la salud y la seguridad de los empleados**.

Entre los beneficios más destacados se encuentran:

- **Reducción de accidentes laborales:** Los EPP minimizan el impacto de riesgos como caídas, cortes o exposición a sustancias peligrosas.
- **Cumplimiento normativo:** El uso adecuado de EPP ayuda a las empresas a cumplir con estándares de seguridad como la **ISO 45001** y regulaciones locales.
- **Protección de la salud a largo plazo:** Algunos riesgos, como el ruido o la exposición a agentes químicos, pueden tener efectos acumulativos. Los EPP previenen enfermedades ocupacionales crónicas.

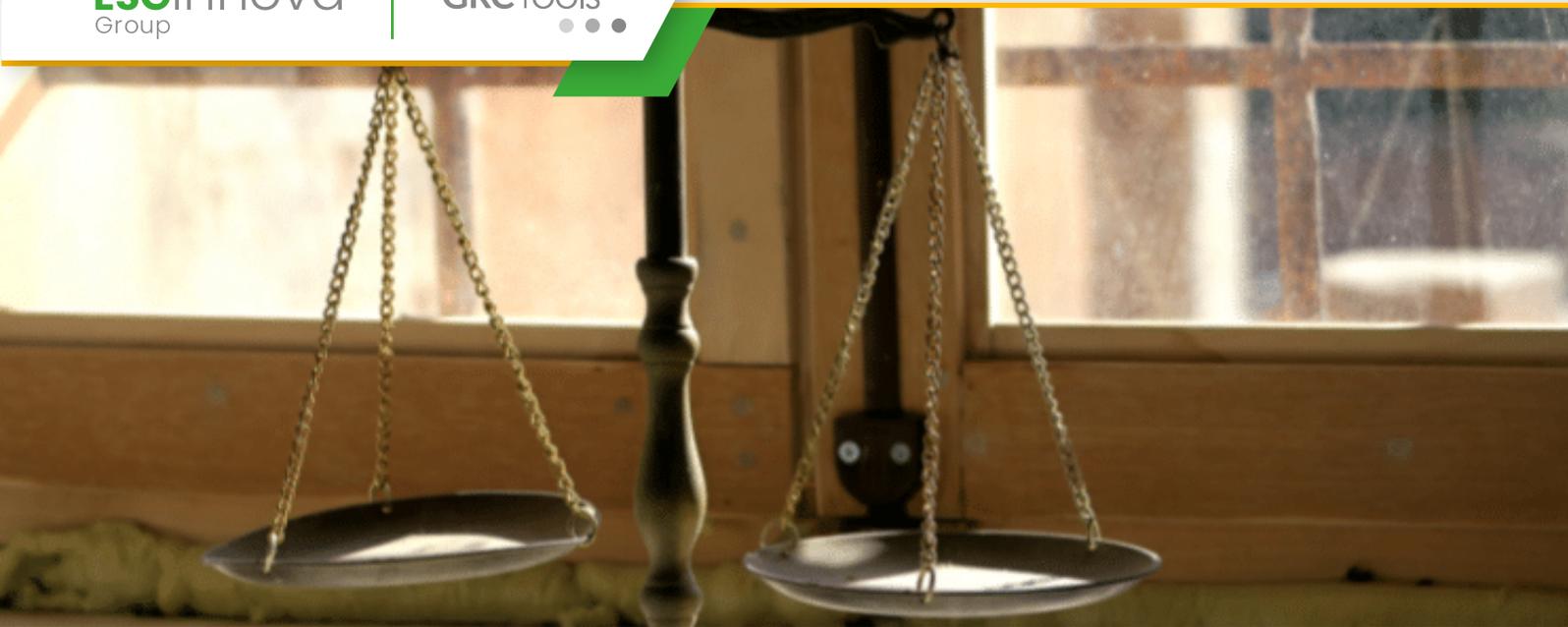
Tipos de elementos de protección personal

Los EPP se clasifican en diferentes **tipos** según la parte del cuerpo que protegen y los **riesgos que mitigan**.

GRCTools



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



¿Qué significan las siglas BSC?

El término **BSC** hace referencia al **Balanced Scorecard**, una herramienta de **gestión estratégica** desarrollada por Robert Kaplan y David Norton en la década de 1990. En español, se conoce como **Cuadro de Mando Integral (CMI)**. Este método permite a las organizaciones traducir su visión y estrategia en un conjunto equilibrado de indicadores que **evalúan el desempeño de manera integral**.

El **BSC** no solo se centra en los **resultados financieros**, sino que también incorpora **aspectos no financieros**, como procesos internos, aprendizaje y desarrollo, y relaciones con los clientes. En este artículo, exploraremos qué es el Balanced Scorecard, cómo funciona, y sus beneficios para la gestión estratégica.

BSC

- El **Balanced Scorecard** es una **metodología que ayuda a las organizaciones a medir y gestionar su desempeño a través de un enfoque balanceado**. Este balance se logra al considerar cuatro **perspectivas** fundamentales:

- **Perspectiva financiera:** Evalúa el rendimiento económico.
- **Perspectiva del cliente:** Analiza la satisfacción y fidelización de los clientes.
- **Perspectiva de procesos internos:** Identifica la eficiencia de los procesos operativos.
- **Perspectiva de aprendizaje y crecimiento:** Mide la capacidad de innovación, formación y mejora continua.

Origen del BSC:

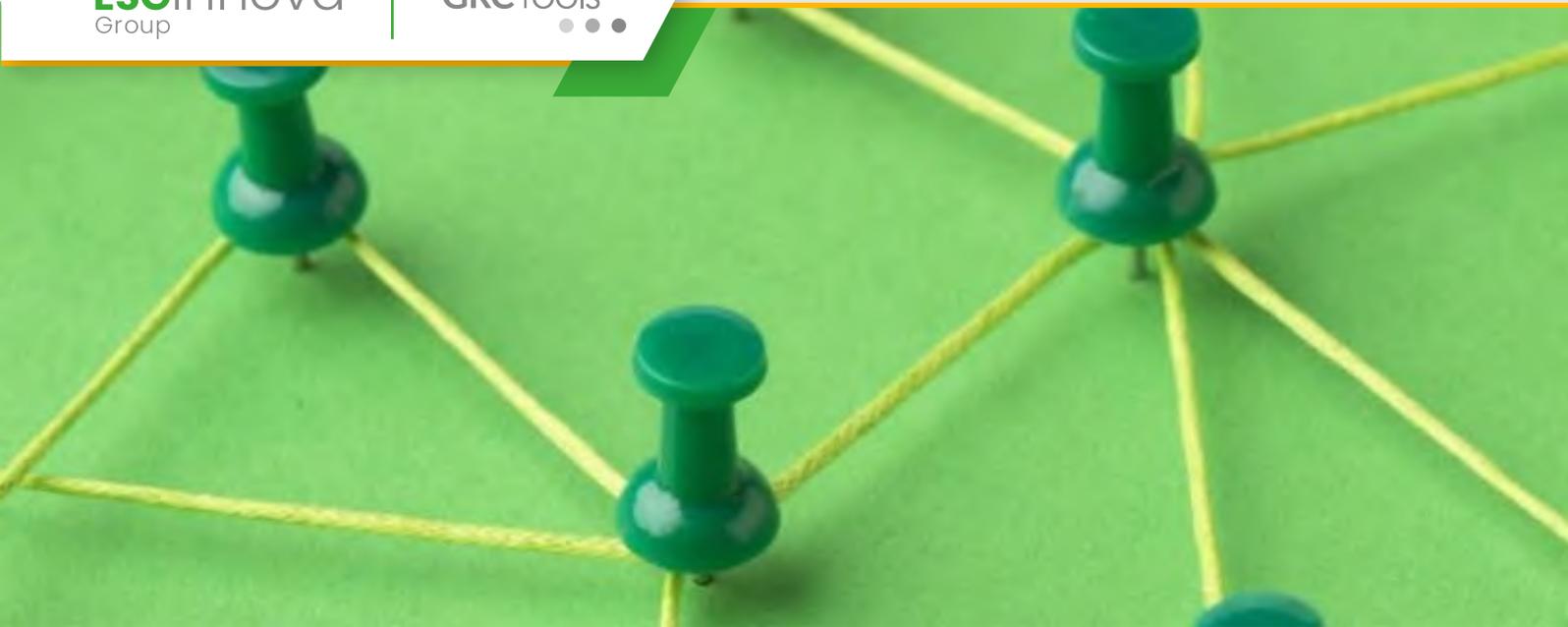
Kaplan y Norton desarrollaron este modelo para **superar las limitaciones de las métricas financieras tradicionales**. Su propuesta fue integrar **aspectos cualitativos y cuantitativos**, permitiendo una **visión más holística** del desempeño organizacional.

Importancia del BSC en la gestión estratégica

El **Balanced Scorecard** es una herramienta crucial para **transformar la visión y misión** de una empresa en **acciones concretas**. Su enfoque multidimensional permite **alinearse a toda la organización** hacia objetivos comunes.

Beneficios clave del BSC:

- ❖ **Visión integral:** Proporciona un panorama claro de todos los aspectos importantes para el éxito organizacional.
- ❖ **Alineación estratégica:** Ayuda a conectar las actividades diarias con los objetivos estratégicos.



¿Qué es un mapa estratégico en Balanced Scorecard?

El **Balanced Scorecard (BSC)** es una herramienta de gestión estratégica que permite a las organizaciones traducir su visión y estrategia en objetivos concretos y medibles. En este contexto, el **mapa estratégico** emerge como un componente clave, proporcionando una representación visual de cómo los diferentes objetivos estratégicos están interconectados y contribuyen al éxito global de la organización.

¿Qué es un mapa estratégico?

Un **mapa estratégico** es un diagrama que organiza y muestra las relaciones entre los objetivos estratégicos de una empresa a través de cuatro perspectivas principales:

- 01. Financiera:** Se enfoca en los resultados económicos y la creación de valor para los accionistas.
- 02. Clientes:** Analiza cómo la organización debe posicionarse para satisfacer las necesidades del cliente y generar ventajas competitivas.

03. Procesos internos: Evalúa los procesos críticos que deben optimizarse para alcanzar los objetivos financieros y de cliente.

04. Aprendizaje y crecimiento: Examina la capacidad de la organización para innovar, mejorar y aprender.

Estas perspectivas están interconectadas, lo que permite visualizar cómo las acciones en un área impactan en otras. Por ejemplo, invertir en capacitación (aprendizaje y crecimiento) puede mejorar la eficiencia de los procesos internos, lo que a su vez incrementa la satisfacción del cliente y, finalmente, mejora los resultados financieros.

Beneficios de un mapa estratégico en Balanced Scorecard

La implementación de un **mapa estratégico** aporta múltiples beneficios a las empresas:

- ❖ **Claridad en la estrategia:** Proporciona una visión estructurada y clara de los objetivos estratégicos.
- ❖ **Alineación organizacional:** Facilita la alineación de los departamentos y equipos con los objetivos globales.
- ❖ **Seguimiento del rendimiento:** Permite medir el progreso y ajustar las acciones según sea necesario.
- ❖ **Toma de decisiones informada:** Mejora la capacidad para tomar decisiones basadas en datos y resultados esperados.



3 Claves para hacer un Mapa Estratégico

El **mapa estratégico** es una herramienta visual clave para las organizaciones que buscan **alinear sus objetivos estratégicos con sus actividades operativas**. Popularizado por Kaplan y Norton en el marco del **Balanced Scorecard (BSC)**, este enfoque permite **comprender y comunicar la estrategia** empresarial de forma clara y efectiva.

Un **mapa estratégico** ayuda a **conectar los diferentes objetivos** de una organización mediante **relaciones causa-efecto**. Además, su diseño facilita la **identificación de áreas críticas de mejora** y oportunidades para maximizar el rendimiento. En este artículo, exploraremos tres claves esenciales para crear un mapa estratégico exitoso.

Mapa estratégico

Un **mapa estratégico** es una **representación gráfica de los objetivos estratégicos de una organización**, estructurada en función de las **perspectivas del Balanced Scorecard**: financiera,

cliente, procesos internos, y aprendizaje y crecimiento. Este enfoque permite a las empresas visualizar cómo cada objetivo contribuye al **logro de su misión y visión**.

Importancia del mapa estratégico:

El valor de un **mapa estratégico** radica en su capacidad para:

- **Alinear equipos y departamentos** hacia metas comunes.
- Identificar **interdependencias** entre los objetivos estratégicos.
- **Mejorar la comunicación** de la estrategia en todos los niveles organizativos.

Clave 1: Definir claramente la visión y los objetivos estratégicos

El primer paso para crear un mapa estratégico efectivo es tener **claridad sobre la misión, visión y los objetivos** estratégicos de la organización. Sin esta base sólida, es imposible desarrollar un **plan coherente**.

1.1 Establecer la visión y misión

- La **visión** describe a dónde quiere llegar la organización en el largo plazo.
- La **misión** define el propósito y el valor que ofrece la empresa a sus stakeholders.



¿Qué dice la Ley 21663 de Chile?

En el actual contexto de transformación digital, la ciberseguridad se posiciona como una prioridad fundamental para la protección de empresas y sectores críticos. En **Chile**, la promulgación de la **Ley 21663: Ley Marco de Ciberseguridad**, en 2023 y homologada el 8 de abril de 2024, representa un paso histórico hacia la protección de infraestructuras críticas y de información sensible frente a ciberamenazas. Esta normativa, diseñada e implementada por la **Agencia de Ciberseguridad de Chile**, establece directrices específicas para fortalecer la seguridad de diversos sectores considerados esenciales para el funcionamiento del país.

Entre los sectores alcanzados por esta legislación destacan el sector público, telecomunicaciones, energía, transportes, salud y financiero. Todos ellos deben adherirse a estrictas medidas de protección que incluyan evaluaciones de riesgos, implementación de políticas de seguridad, capacitación del personal y una gestión adecuada de incidentes. Pero, ¿cuáles son los **retos específicos** que enfrenta el sector empresarial en este nuevo marco?

Los problemas del sector empresarial frente a la Ley 21663

A pesar de la importancia de la **Ley 21663**, muchas empresas enfrentan serios desafíos para cumplir con sus requerimientos. Entre los problemas más comunes destacan:

- 01. Falta de concienciación interna:** En muchas organizaciones, la ciberseguridad no se percibe como una prioridad estratégica, lo que limita el compromiso de los directivos y empleados.
- 02. Recursos limitados:** Especialmente en pequeñas y medianas empresas, los recursos financieros y humanos destinados a la ciberseguridad suelen ser insuficientes.
- 03. Complejidad técnica:** Adoptar las medidas exigidas por la normativa puede ser complicado para empresas sin personal capacitado en gestión de riesgos o tecnologías de seguridad.
- 04. Cumplimiento legal:** La falta de conocimiento sobre las obligaciones legales y los plazos establecidos puede derivar en sanciones severas que oscilan entre 5.000 y 40.000 UTM, equivalentes a 260.000 € y 330.000 €.
- 05. Gestión de incidentes:** Muchas empresas no cuentan con planes de respuesta a incidentes ni equipos especializados para actuar rápidamente, como exige la normativa, que establece un plazo de apenas tres horas para notificar eventos al CSIRT Nacional.

Estos retos dificultan el cumplimiento de la ley y además exponen a las empresas a **riesgos** significativos, desde pérdida de datos hasta daños reputacionales y financieros.



¿Qué significan las siglas ERM?

La gestión de riesgos empresariales, conocida como **ERM** por sus siglas en inglés (*Enterprise Risk Management*), es un enfoque integral diseñado para identificar, evaluar y gestionar los riesgos que enfrentan las organizaciones en su camino hacia el cumplimiento de objetivos.

Se trata de un marco que abarca toda la organización, permitiendo a las empresas reaccionar ante **riesgos potenciales** y también anticiparse a ellos, convirtiendo la gestión de riesgos en una **ventaja competitiva**. Este enfoque considera todos los tipos de riesgos, desde financieros y operativos hasta reputacionales y tecnológicos, garantizando que las decisiones estratégicas estén alineadas con la tolerancia al riesgo de la empresa.

Las empresas se enfrentan diariamente a operaciones complejas, llenas de incertidumbres y regulaciones cambiantes, el ERM se ha convertido en una herramienta estratégica para garantizar la **sostenibilidad** y el **crecimiento**.

Pero, ¿cómo impactan estos riesgos en el sector empresarial y qué soluciones ofrece la tecnología para abordarlos?

Los problemas del sector empresarial en la gestión de riesgos

El sector empresarial enfrenta una variedad de desafíos relacionados con la gestión de riesgos, que pueden derivar en costos significativos, daños reputacionales e incluso problemas legales.

Algunos de los **problemas más comunes** incluyen:

1. Falta de visibilidad integral

Muchas empresas gestionan los riesgos de forma aislada, sin una visión centralizada. Esto genera **duplicidad de esfuerzos** y dificulta la toma de decisiones basada en datos.

2. Procesos manuales y desactualizados

Dependencia de hojas de cálculo y métodos manuales que no solo son propensos a errores, sino que también **limitan la capacidad de respuesta** ante riesgos emergentes.

3. Cumplimiento normativo desorganizado

Con regulaciones que varían entre industrias y países, **mantener el cumplimiento es un reto constante**, especialmente sin herramientas que automaticen y estandaricen procesos.



Cuáles son los objetivos estratégicos de una empresa y cuál es su importancia

En el mundo empresarial, los **objetivos estratégicos** son el punto de partida para el **éxito organizacional**. Estas metas permiten a las empresas establecer un rumbo claro, **alineando recursos y esfuerzos** hacia la consecución de resultados medibles. Sin estos bien definidos, las organizaciones corren el riesgo de **operar sin un propósito claro, perdiendo competitividad** en un mercado cada vez más exigente.

Este artículo explora qué son los **objetivos estratégicos**, su importancia, y cómo establecerlos de manera efectiva para impulsar el crecimiento y la sostenibilidad empresarial.

Objetivos estratégicos

Los **objetivos estratégicos** son **metas a largo plazo** que definen hacia **dónde quiere dirigirse una organización**. Estos objetivos se desarrollan considerando la **misión y visión empresarial**, así como

las condiciones del entorno competitivo y las capacidades internas de la empresa.

Características de los objetivos estratégicos

- Para ser efectivos, deben cumplir ciertas **características**:
- **Claridad**: Deben estar definidos de manera precisa y comprensible.
- **Medibles**: Es crucial que exista un método para evaluar su progreso.
- **Alcanzables**: Aunque desafiantes, deben ser realistas según los recursos disponibles.
- **Relevantes**: Deben alinearse con la misión y visión de la empresa.
- **Temporales**: Especificar un marco de tiempo para su consecución es esencial.

Importancia de los objetivos estratégicos

Alineación de recursos y esfuerzos

Los **objetivos estratégicos** actúan como un marco para la **toma de decisiones**.

Ayudan a **priorizar proyectos y asignar recursos** de manera eficiente, asegurando que todas las áreas de la organización trabajen en conjunto hacia un **propósito común**.



¿Cómo implementar los OKR en tu proyecto empresarial?

Los **OKR** (Objectives and Key Results) se han convertido en una **metodología** clave para la **gestión estratégica** y la mejora del **rendimiento** en las organizaciones. Su implementación es fundamental para aquellas empresas que buscan alinear sus esfuerzos, optimizar sus recursos y lograr resultados medibles. Comprender los pasos para integrar esta metodología en un proyecto empresarial es esencial para abordar los desafíos actuales del sector, como la falta de claridad en los objetivos, la desconexión entre equipos y la dificultad para medir el éxito.

Además, contar con herramientas tecnológicas como el **Software OKR** de **GRCTools** puede marcar la diferencia al proporcionar una plataforma que **simplifica la gestión estratégica** y asegura que cada meta trazada se traduzca en **resultados tangibles** y **sostenibles**.

Los problemas del sector empresarial: La necesidad de claridad y enfoque

Uno de los problemas más serios a los que se enfrentan las organizaciones se traduce en una serie de retos que dificultan alcanzar sus objetivos y mantener un crecimiento sostenible. Algunos de los **problemas más comunes** incluyen:

1. Falta de alineación entre equipos y objetivos

En muchas empresas, los departamentos **trabajan de manera aislada**, lo que genera una **desconexión** entre los **objetivos estratégicos** de la organización y las **actividades** diarias de los equipos.

2. Metas poco claras o no medibles

Establecer **objetivos vagos** o **sin indicadores** claros de éxito dificulta medir el progreso y tomar decisiones basadas en datos.

3. Escasez de herramientas para el seguimiento

Las empresas suelen confiar en hojas de cálculo o sistemas manuales para monitorear el progreso, lo que no solo **consume tiempo**, sino que también aumenta el **riesgo de errores**.

4. Dificultad para adaptarse a cambios rápidos

El mercado evoluciona constantemente, y las organizaciones necesitan herramientas que les permitan **recalibrar sus objetivos de manera ágil y precisa**.



Importancia de la flexibilidad de la planeación operativa ante los cambios

La capacidad de adaptarse a los cambios es un atributo esencial para las organizaciones, por ello, la **planeación operativa** es un eje fundamental de la gestión empresarial. Esta debe ser lo suficientemente flexible para responder rápidamente a los retos del entorno.

Vamos a introducirnos en los principales problemas que enfrentan las empresas en este contexto y cómo la implementación de tecnologías avanzadas, como el Software de **Inspecciones y Control Operacional** de **GRCTools**, puede ser clave para superarlos.

Componentes clave de la planeación operativa

La **planeación operativa** se refiere a la capacidad de una organización para adaptarse, responder y ajustarse de manera ágil a los cambios internos y externos que afectan sus operaciones. Esto implica modificar recursos, procesos, estrategias y prioridades

para afrontar situaciones dinámicas sin comprometer la eficiencia ni la calidad de los resultados.

En esencia, la planeación operativa permite a las empresas manejar imprevistos, aprovechar oportunidades emergentes y minimizar los impactos de eventos disruptivos, como cambios en la demanda, nuevas regulaciones, innovaciones tecnológicas o crisis económicas.

- **Capacidad de respuesta:** Rapidez con la que una organización puede identificar y reaccionar a los cambios.
- **Adaptabilidad de recursos:** Habilidad para redistribuir personal, materiales, tecnología o presupuestos según sea necesario.
- **Resiliencia:** Aptitud para recuperarse rápidamente de interrupciones o contratiempos operativos.
- **Innovación continua:** Capacidad para actualizar procesos y adoptar tecnologías que mejoren la adaptabilidad.
- **Colaboración interdepartamental:** Integración efectiva entre áreas para garantizar la coherencia en las respuestas a los cambios.

Ejemplo práctico de flexibilidad operativa

Una empresa de manufactura que utiliza sistemas de producción ajustados (como **Just-in-Time**) puede adaptar su capacidad para responder rápidamente a aumentos o disminuciones en la demanda, evitando tanto el exceso de inventario como la falta de suministros. Esto es posible gracias a sistemas que monitorean en tiempo real y permiten ajustar las operaciones según las necesidades actuales.



5 ejemplos de Balanced Scorecard de una empresa

El **Balanced Scorecard (BSC)** es una herramienta estratégica que permite a las empresas **alinear sus objetivos con sus actividades diarias**, midiendo el **desempeño** en áreas clave como finanzas, clientes, procesos internos y aprendizaje organizacional. En este artículo, exploraremos **5 ejemplos prácticos de Balanced Scorecard de una empresa**, destacando cómo esta metodología puede transformar la gestión estratégica.

Balanced Scorecard de una empresa

El **Balanced Scorecard (BSC)** es un **modelo de gestión** desarrollado por Robert Kaplan y David Norton, diseñado para proporcionar una **visión integral del desempeño** organizacional. A diferencia de los métodos tradicionales que se enfocan únicamente en **métricas financieras**, el BSC considera cuatro **perspectivas**:

- ❖ **Financiera**: Evalúa el impacto económico de las estrategias implementadas.

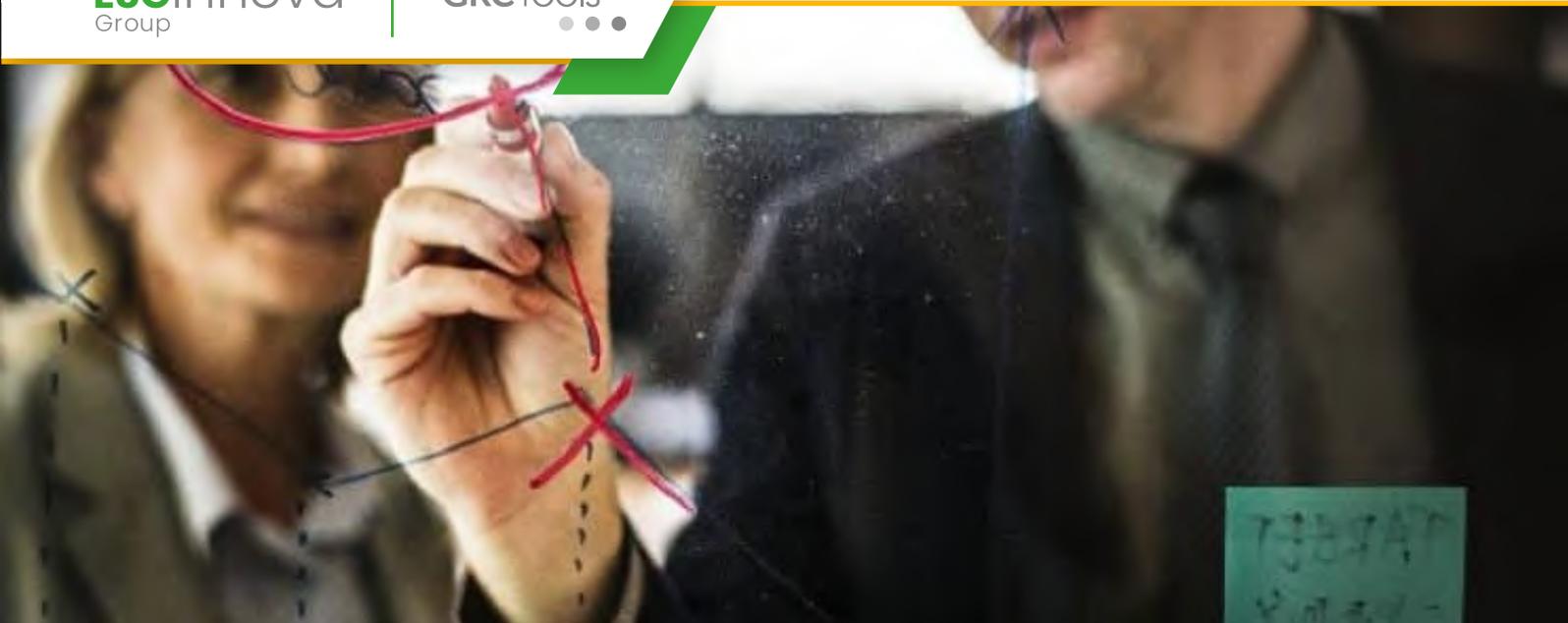
- ❖ **Clientes:** Mide la satisfacción y fidelización de los clientes.
- ❖ **Procesos internos:** Analiza la eficiencia y efectividad de las operaciones internas.
- ❖ **Aprendizaje y crecimiento:** Se enfoca en el desarrollo del talento humano y la innovación.

5 ejemplos de Balanced Scorecard en empresas

1. Balanced Scorecard en el sector retail

Las empresas de retail, como supermercados o tiendas de ropa, necesitan satisfacer a los clientes mientras optimizan sus costos operativos. Un ejemplo de BSC para este sector podría incluir:

- **Perspectiva financiera:** Incrementar un 10% las ventas trimestrales.
- **Perspectiva de clientes:** Mejorar la experiencia de compra reduciendo los tiempos de espera en caja en un 20%.
- **Perspectiva de procesos internos:** Optimizar la gestión de inventarios para evitar roturas de stock.
- **Perspectiva de aprendizaje y crecimiento:** Capacitar al 80% del personal en atención al cliente.



Cómo mejorar tu gestión con un Cuadro de Mando BSC

Entre los desafíos a los que se enfrentan las organizaciones podemos destacar desde la necesidad de mantener la **rentabilidad**, hasta alinear a los equipos con los **objetivos** y la **gestión estratégica** eficaz. De ahí la necesidad de contar con herramientas específicas para abordar esta serie de problemáticas.

El **Balanced Scorecard**, o **Cuadro de Mando BSC**, se convierte en esa herramienta poderosa para transformar la forma en que las empresas gestionan sus operaciones y miden su éxito. Vamos a explorar cómo el uso de un cuadro de mando puede resolver problemas comunes del sector empresarial y cómo la plataforma tecnológica **GRCTools** optimiza esta implementación mediante su software especializado.

Los problemas del sector empresarial que dificultan la gestión

1. Falta de alineación entre estrategia y operación

Muchas organizaciones enfrentan el desafío de alinear las **actividades diarias** con los **objetivos estratégicos**. Las decisiones operativas a menudo se toman **sin una visión clara** de cómo contribuyen a los resultados finales, generando inconsistencias y esfuerzos dispersos.

2. Dificultades en el seguimiento de los indicadores clave de rendimiento (KPIs)

En muchas empresas, la monitorización de los **KPIs** se realiza de manera **manual** o **desorganizada**, lo que dificulta medir el progreso y anticiparse a problemas potenciales.

3. Desconexión entre áreas y departamentos

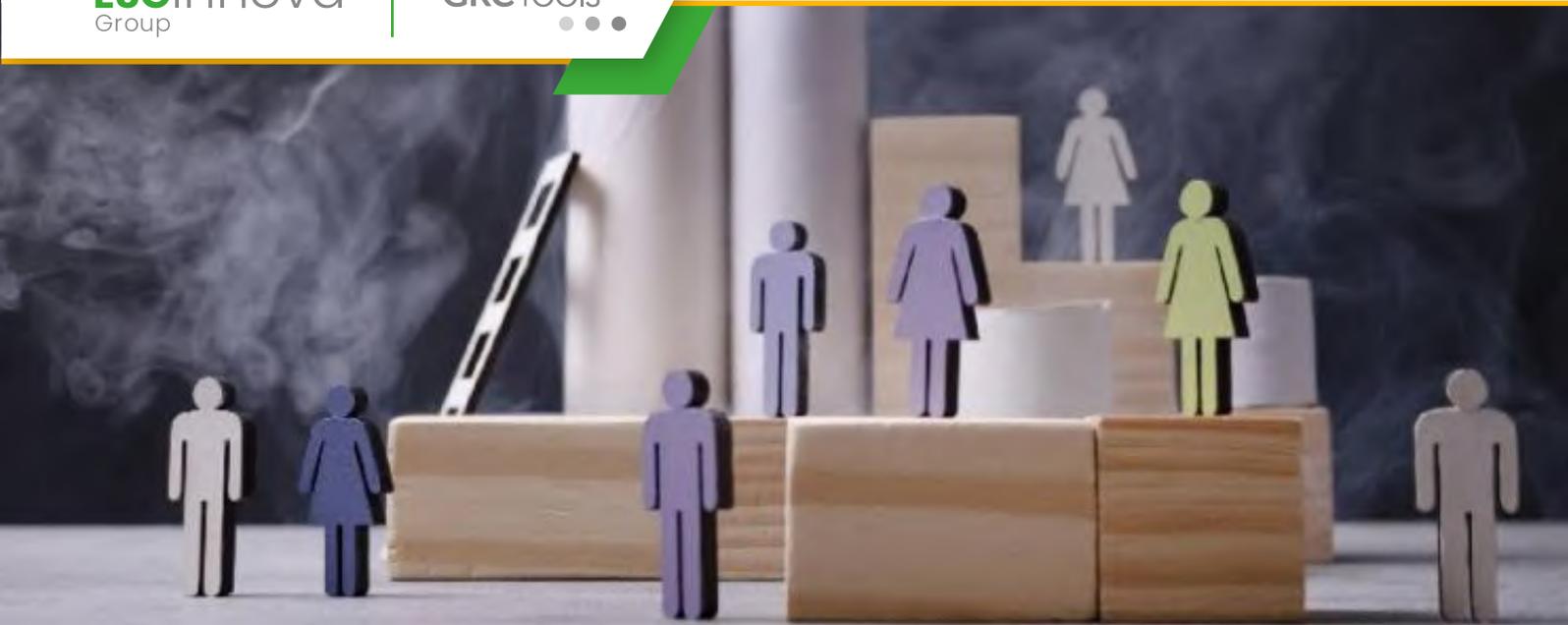
Los silos organizacionales siguen siendo un problema recurrente. La **falta de comunicación** y **colaboración** entre departamentos puede obstaculizar el logro de objetivos comunes y generar redundancias.

4. Falta de datos fiables para la toma de decisiones

La toma de decisiones basada en datos es fundamental, pero muchas organizaciones carecen de sistemas que integren **información precisa y oportuna**, lo que puede llevar a **decisiones incorrectas o poco fundamentadas**.

5. Resistencia al cambio y adopción de tecnología

Adoptar nuevas herramientas y enfoques puede ser un reto para equipos **acostumbrados a trabajar con procesos tradicionales**, lo que ralentiza la transformación organizacional.



Guía para elaborar un Cuadro de Mando Integral Balanced Scorecard

El **Cuadro de Mando Integral Balanced Scorecard**, es una herramienta clave para transformar la estrategia empresarial en acciones concretas y medibles. En un contexto corporativo donde las empresas enfrentan entornos complejos y demandantes, el CMI se posiciona como una **metodología** esencial para alinear los objetivos estratégicos con las operaciones del día a día. Sin embargo, su implementación puede estar llena de desafíos, especialmente para organizaciones en sectores altamente regulados o con estructuras complejas.

A continuación, exploraremos **cómo elaborar un Cuadro de Mando Integral Balanced Scorecard**, los problemas más comunes que enfrenta el sector empresarial y cómo la tecnología puede ser el aliado clave en este proceso.

Problemas comunes del sector empresarial al gestionar el desempeño

En el sector empresarial, la gestión del desempeño suele estar plagada de retos derivados de la **falta de alineación, visibilidad y herramientas** adecuadas para medir el avance hacia los objetivos. Algunos de los problemas más comunes incluyen:

1. Falta de alineación entre la estrategia y las operaciones

Muchas organizaciones desarrollan planes estratégicos que no se traducen en acciones concretas a nivel operativo. Esto genera una **desconexión** entre las metas de alto nivel y el trabajo diario de los equipos.

2. Exceso de datos y poca claridad

Con la digitalización, las empresas generan **grandes volúmenes de datos**, pero carecen de sistemas eficaces para filtrar, analizar y convertir esta información en conocimiento accionable.

3. Dificultad para medir el impacto de los objetivos estratégicos

En muchos casos, los **indicadores clave de desempeño (KPIs)** seleccionados no reflejan adecuadamente el progreso hacia los objetivos, lo que complica la toma de decisiones.

4. Rigidez de los sistemas tradicionales

Las herramientas tradicionales, como **hojas de cálculo** o **procesos manuales**, limitan la agilidad y dificultan la adaptación a cambios rápidos en el entorno empresarial.



7 ejemplos para hacer un análisis de riesgos

Analisis de riesgos

El **análisis de riesgos** es una metodología esencial que permite a las organizaciones **identificar, evaluar y gestionar posibles amenazas** que podrían **afectar sus operaciones, activos o reputación**. Este proceso sistemático **facilita la toma de decisiones informadas y la implementación de medidas preventivas** para mitigar o eliminar dichos riesgos.

Según la información disponible en la página de GRCTools, el análisis de riesgos implica una serie de **pasos clave**:

- 01. Identificación de riesgos:** Detectar todas las posibles amenazas que podrían impactar negativamente a la organización.
- 02. Evaluación de riesgos:** Analizar la probabilidad de ocurrencia y el impacto potencial de cada riesgo identificado.
- 03. Priorización de riesgos:** Clasificar los riesgos según su nivel de

severidad y la urgencia con la que deben ser abordados.

- 04. Desarrollo de estrategias de mitigación:** Establecer planes y acciones específicas para reducir la probabilidad de ocurrencia o el impacto de los riesgos priorizados.
- 05. Monitoreo y revisión:** Supervisar continuamente los riesgos y la efectividad de las estrategias implementadas, realizando ajustes cuando sea necesario.

Implementar un análisis de riesgos efectivo permite a las organizaciones **anticiparse a posibles problemas, optimizar recursos** y asegurar la **continuidad de sus operaciones**, fortaleciendo así su resiliencia y **capacidad de respuesta** ante situaciones adversas.

7 ejemplos para hacer una buena gestión de riesgos

1. Análisis de riesgos en la gestión de proyectos

Al planificar un proyecto, es fundamental **identificar riesgos** asociados al presupuesto, los plazos, y la calidad de los entregables.

- **Paso 1:** Identificar riesgos específicos, como retrasos en la entrega de materiales.
- **Paso 2:** Evaluar el impacto en el cronograma y el costo.
- **Paso 3:** Desarrollar un plan de contingencia, como mantener proveedores alternativos.



Formas de alcanzar el éxito gracias a una matriz de riesgos

Contar con una **matriz de riesgos bien estructurada** permite identificar vulnerabilidades, tomar decisiones informadas y crear estrategias para mitigar amenazas. Vamos a tratar los problemas comunes que enfrenta el sector empresarial y cómo el **Software de Gestión de Riesgos de GRCTools** puede ser un aliado clave para superarlos.

En la mayoría de las ocasiones, el éxito de una empresa no depende exclusivamente de su capacidad para innovar y satisfacer las necesidades de sus clientes. Hay que destacar la importancia de **anticiparse a los riesgos y gestionarlos de manera efectiva**, ya que el entorno actual es cambiante y lleno de incertidumbres.

Los clientes valoran que una empresa tenga la capacidad de anticiparse a los riesgos, ya que eso demuestra **responsabilidad y compromiso** con la continuidad del negocio.

La matriz de riesgos

Una matriz de riesgos se compone de varios elementos fundamentales que permiten identificar, evaluar y gestionar los riesgos de manera efectiva dentro de una organización. En primer lugar, encontramos la **identificación de riesgos**, donde se definen las posibles amenazas que podrían afectar los objetivos del negocio. A continuación, se realiza la **evaluación del impacto y la probabilidad**, asignando un nivel a cada riesgo en función de su gravedad y la posibilidad de que ocurra.

Esto da lugar a una clasificación que ayuda a priorizar los riesgos. Otro componente clave es la **definición de medidas de mitigación**, donde se establecen acciones concretas para reducir la probabilidad o el impacto de los riesgos. Finalmente, la matriz de riesgos también incluye un **sistema de monitoreo y revisión continua**, que permite actualizar la información sobre los riesgos y evaluar la efectividad de las medidas implementadas. Esta estructura integral permite a las organizaciones tomar decisiones informadas y actuar de manera proactiva frente a las incertidumbres del entorno empresarial.

Problemas comunes en la Gestión de Riesgos empresariales

1. Falta de visibilidad sobre los riesgos

Muchas organizaciones no cuentan con un enfoque estructurado para **identificar, evaluar y monitorear riesgos**. Esto conduce a una toma de decisiones reactiva en lugar de proactiva.



Ley federal de protección de datos personales de México

La **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)** es una pieza clave dentro del marco legal mexicano que busca garantizar la privacidad y seguridad de la información personal. Con la creciente digitalización y la transformación digital de las empresas, el cumplimiento de esta normativa se ha vuelto fundamental para asegurar la confianza de los clientes y evitar sanciones.

¿Qué es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares?

- La **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**, promulgada en 2010, tiene como objetivo principal regular el tratamiento de datos personales por parte de particulares, incluyendo personas físicas y morales que actúan con fines comerciales. La ley establece principios y deberes que deben ser respetados para garantizar el derecho a la privacidad de las personas. Entre sus disposiciones más relevantes, destacan:

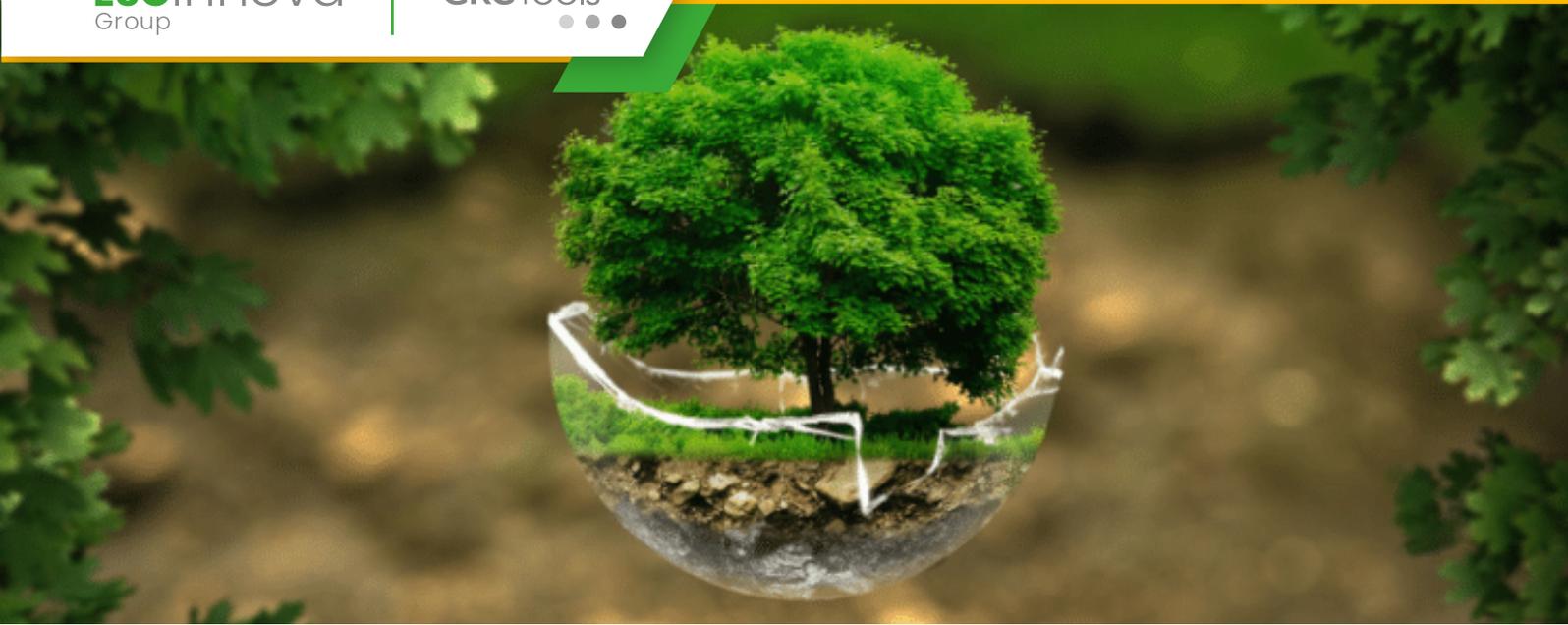
- **Consentimiento:** Las empresas deben obtener el consentimiento del titular de los datos para su tratamiento.
- **Finalidad:** Los datos personales solo pueden ser utilizados para los fines autorizados.
- **Transparencia:** Las empresas deben informar claramente a los titulares sobre el tratamiento de sus datos.
- **Seguridad:** Es obligatorio implementar medidas de seguridad para proteger la información.
- **Derechos ARCO:** Los titulares tienen derecho a Acceder, Rectificar, Cancelar y Oponerse al tratamiento de sus datos personales.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (**INAI**) es la autoridad encargada de supervisar y hacer cumplir esta ley.

Desafíos del Sector Empresarial en la Protección de Datos Personales

Las empresas en México se enfrentan a diversos problemas relacionados con la gestión de la **seguridad de la información** y protección de datos personales, entre los que destacan:

- ❖ **Falta de conciencia y cultura de protección de datos**
- ❖ Muchas organizaciones no comprenden completamente la importancia de proteger los datos personales. Esto lleva a brechas de seguridad y riesgos legales.



¿Cuántos tipos de riesgos ambientales existen para una empresa?

Los **riesgos ambientales** se refieren a cualquier **amenaza o evento que pueda alterar el equilibrio ecológico o la calidad del entorno natural**, afectando directamente a la actividad de una empresa. Estos riesgos pueden tener **implicaciones** serias no solo en el **medio ambiente**, sino también en la **reputación**, la **sostenibilidad** y la **rentabilidad** de las organizaciones. Entender los **tipos de riesgos ambientales** a los que una empresa puede estar expuesta es fundamental para adoptar **prácticas responsables** y cumplir con las **normativas ambientales vigentes**. En este artículo, exploraremos los diferentes tipos de riesgos ambientales y cómo gestionarlos.

Tipos de riesgos ambientales en una empresa

Los **riesgos ambientales** son diversos y pueden **clasificarse en diferentes categorías**. A continuación, describimos los **tipos** principales de **riesgos** que una empresa podría enfrentar.

Riesgos físicos

Los **riesgos físicos** son aquellos que están **directamente relacionados con eventos o cambios en el entorno natural** que pueden afectar la operación de una empresa. Estos riesgos pueden derivar de **fenómenos meteorológicos** extremos, así como de otros **eventos climáticos y geológicos**.

El **cambio climático** ha incrementado la **frecuencia e intensidad** de fenómenos meteorológicos extremos, como tormentas, inundaciones y olas de calor. Las empresas que operan en zonas vulnerables pueden **enfrentarse** a:

- **Daños en infraestructuras:** Las tormentas y las inundaciones pueden afectar los edificios y la maquinaria.
- **Interrupciones en la cadena de suministro:** Los desastres naturales pueden interrumpir el suministro de recursos esenciales o afectar el transporte.
- **Desastres provocados por olas de calor:** Pueden afectar la productividad y la salud de los trabajadores.

Los **terremotos, deslizamientos de tierra y tsunamis** son **riesgos geológicos** que pueden destruir instalaciones, interrumpir la producción y tener efectos devastadores en el medio ambiente cercano.

Las empresas que operan en áreas propensas a estos desastres deben **implementar medidas preventivas y planes de contingencia** para mitigar los efectos de estos eventos.



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.





ESGinnova

Group

Córdoba, España

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

Écija, España

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

Santiago de Chile, Chile

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

Lima, Perú

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

Bogotá, Colombia

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

México DF, México

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

