EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

2025

FEBRERO

ESGinnova Group

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

Índice

Índice

ESG Innova Group

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

01. **Salud y bienestar:** Aportando soluciones innovadoras para una gestión eficaz de la salud y seguridad de los colaboradores.

02. **Educación de Calidad:** Contribuyendo con contenido de valor y programas formativos de primer nivel para los líderes del futuro en todo el mundo.

03. **Igualdad de género:** Promoviendo la igualdad de oportunidades entre todos y todas los/as integrantes de la organización, independientemente de sexo, raza, ideología y religión.

04. **Trabajo decente y crecimiento económico:** Ayudando a las organizaciones a ser más eficaces y eficientes, aportando soluciones para la gestión estratégica, táctica y operativa.

05. **Industria, innovación e infraestructura:** Colaborando con soluciones innovadoras para el desarrollo de las organizaciones, orientándolas a ejercer un impacto positivo en criterios ESG.

06. **Producción y consumo responsables:** Haciendo más eficiente el empleo de recursos por parte de las organizaciones, ayudándoles a mejorar en el largo plazo.

07. **Acción por el clima:** Apoyando a nuestros clientes a reducir sus emisiones y desperdicios de recursos y extraer más rendimiento.

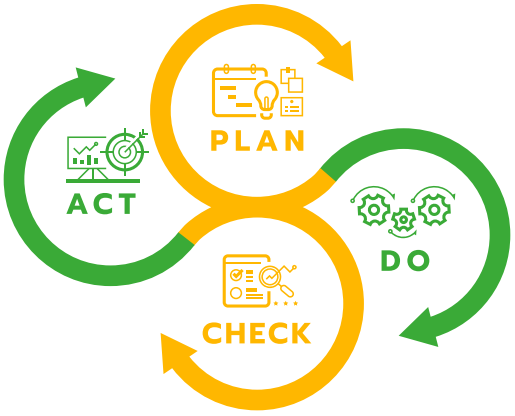
Plataforma ESG Innova

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

❖ Motor de mejora continua

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

ESGinnova Group



❖ Plan

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

❖ Do

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

❖ Check

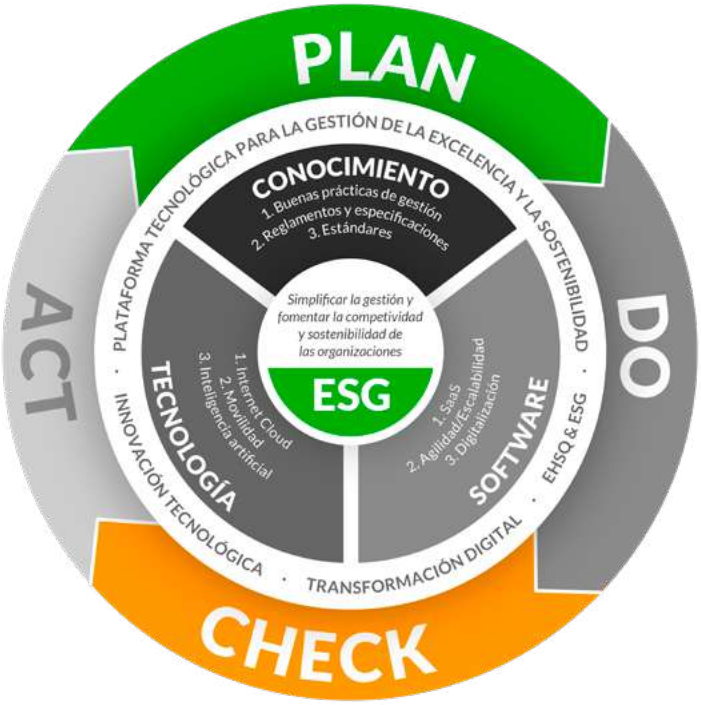
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ Act

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

Unidades de negocio

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



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

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

Unidades de negocio

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

ISOTools

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

HSETools

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

GRCTools

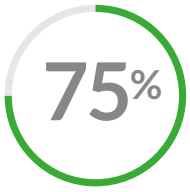
Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento.

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

Menos de tiempo de resolución de una acción correctiva

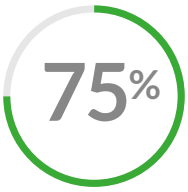
Menos de tiempo de preparación de las reuniones de gestión



Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

Menos de intercambios de documentación física entre sedes y dptos.



Menos de costes indirectos derivados de la gestión documental

La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento

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

Más capacidad de resolución de problemas del sistema de gestión

Más de trabajadores implicados en la gestión del sistema

ESGinnova Group

ISOTools

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

Obtener la certificación ISO 42001: 6 pasos clave para lograrlo

Obtener la certificación ISO 42001 es el paso que sigue tras la implementación exitosa de un sistema de gestión de Inteligencia Artificial. La demostración para la organización, para terceros y para las partes interesadas de que todo se hizo correctamente y la gestión de la IA es ética, legal, transparente y segura es el certificado ISO del sistema.

Obtener la certificación ISO 42001 requiere seguir un proceso. Es un desafío que **requiere realizar acciones que van más allá de solicitar el certificado**. Con la acogida masiva que ha tenido el nuevo **estándar de sistemas de gestión de IA**, es importante conocer y entender la importancia de obtener la certificación ISO 42001 y contar con una guía para hacerlo.

Por qué es importante obtener la certificación ISO 42001

La irrupción de la Inteligencia Artificial en el mundo empresarial, industrial y comercial ha sido apresurada y contundente. Tanto, que **las organizaciones apenas han tiempo de evaluar, y menos gestionar, riesgos**. Esta ausencia de gestión de riesgos generó desconfianza hacia las organizaciones que intentan aprovechar las oportunidades que IA ofrece.

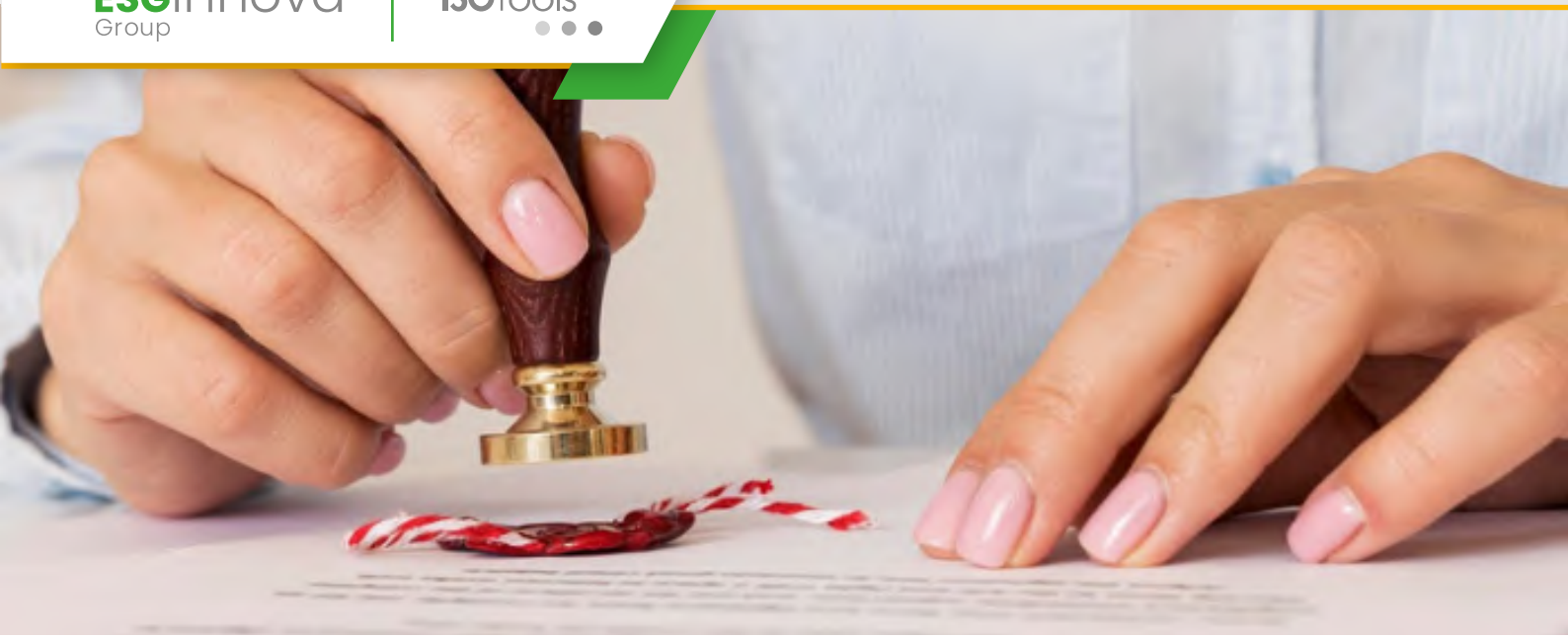
ISO 42001 llega para resolver estos problemas. Se trata del primer estándar de alcance internacional, **diseñado para eliminar o minimizar los riesgos que implica el uso o desarrollo de productos de IA**. Sin embargo, a pesar de la solidez y la eficiencia que demuestra el estándar, es evidente que la **implementación de ISO 42001** por sí sola no resuelve todos los problemas.

Las empresas necesitan obtener la certificación ISO 42001 para gozar de la confianza de sus clientes, de los reguladores y de las personas en general. También la requieren para contar con **herramientas que les permitan adoptar prácticas de gobernanza, riesgo, cumplimiento y sostenibilidad**, necesarias para sobresalir en el mundo corporativo moderno.

Obtener la certificación ISO 42001 **entrega otros interesantes beneficios** a las organizaciones que adoptan el sistema de gestión basado en este estándar:

- **Alinea los objetivos comerciales con la gobernanza de IA**, lo que garantiza un uso responsable, aprovechando las ventajas y oportunidades sin exponer a las personas o a la organización a los riesgos inherentes al uso de esta tecnología.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Qué significa la acreditacion ISO?

La **acreditacion ISO** es un término que cobra cada vez más relevancia, pero, ¿sabes qué implica realmente obtener una acreditación de este tipo? En este artículo, explicaremos su significado, su importancia y cómo puede transformar la gestión de tu empresa.

Acreditacion ISO

La **acreditacion ISO** es un proceso mediante el cual un organismo de certificación independiente verifica que una compañía cumple con los requisitos establecidos en una norma ISO específica. Estas normas, desarrolladas por la Organización Internacional de Normalización (ISO), son reconocidas a nivel global y establecen estándares de **calidad**, **seguridad, eficiencia y sostenibilidad**, entre otros muchos, en diversos sectores.

No debe confundirse con la certificación. Mientras que la certificación es el proceso por el cual una organización demuestra que cumple con una norma, la acreditación es el reconocimiento formal de que el organismo que realiza la certificación es competente y confiable para hacerlo.

En otras palabras, la acreditación es un **respaldo a la credibilidad de la certificación**.

Importancia de la acreditacion ISO

La **acreditacion ISO** no es solo un sello de calidad; es una herramienta estratégica que ofrece múltiples **beneficios para las empresas** como los que se detallan a continuación:

Credibilidad y confianza

La acreditacion ISO demuestra a clientes, proveedores y partes interesadas que **la empresa opera bajo estándares internacionales reconocidos**. Este reconocimiento fortalece la reputación de la organización y genera confianza en sus productos o servicios, lo que se traduce en fidelizar a los clientes y en la atracción de nuevos negocios. Además, en sectores muy regulados, como el médico o el alimentario, la acreditación es casi un requisito indispensable para operar.

Mejora continua con la acreditacion ISO

Las normas ISO están diseñadas para fomentar y optimizar los procesos internos de la empresa. Esto se traduce en **una mayor eficiencia operativa y en una reducción de costos a largo plazo.** La implementación de estas normas obliga a las compañías a revisar y mejorar de forma constante sus procedimientos, lo que contribuye activamente a la innovación y al crecimiento sostenible.

Además, la mejora continua es un principio clave de muchas **normas ISO**, como la ISO 9001 de calidad, lo que asegura que la empresa no se estanque y siempre busque superarse.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Quiénes deben cumplir con el Reglamento de Resiliencia Operativa Digital (DORA)?

El **Reglamento de Resiliencia Operativa Digital** (DORA) es la normativa de la Unión Europea que busca reforzar la **seguridad informática**, cerrar brechas de ciberseguridad y fortalecer, como su título expresa, la resiliencia operativa en empresas del sector financiero.

El Reglamento de Resiliencia Operativa Digital entró en vigor en enero de 2023, pero tiene aplicación práctica para las empresas obligadas a partir de este 2025. DORA permitirá a las organizaciones del sector **resistir, responder y recuperarse ante la presencia de una amenaza, una irrupción o una vulneración** de sus sistemas informáticos y de comunicaciones.

Qué empresas deben cumplir con el Reglamento de Resiliencia Operativa Digital

La **Regulación DORA** es una normativa diseñada para cumplir objetivos en empresas del sector financiero. El Reglamento de Resiliencia Operativa Digital **establece tres grupos de empresas obligadas**. Sin embargo, es importante determinar que no todas tienen las mismas obligaciones.

Es interesante observar que uno de esos tres grupos **se enfoca en organizaciones que no necesariamente pertenecen al sector financiero,** pero sí guardan una relación tangencial con organizaciones financieras.

Qué organizaciones están obligadas a cumplir con el Reglamento de Resiliencia Operativa Digital

El Reglamento de Resiliencia Operativa Digital se aplica para la mayoría de las **organizaciones del sector financiero que operan en la Unión Europea** y que se dividen en dos grupos de acuerdo con su tamaño. El tercer grupo de empresas obligadas a cumplir el Reglamento DORA son las que proveen servicios TIC externos para organizaciones financieras. Los tres grupos son los siguientes:

1. Entidades financieras de gran tamaño obligadas con DORA

Y que tienen a su cargo el cumplimiento de los requisitos plenos. Se trata de todas las organizaciones que **desarrollan las actividades en cualquiera de los países de la Unión Europea**.

Todo lo que tienes que saber sobre el acuerdo entre ISO y la ONU

El acuerdo entre la **Organización Internacional de Normalización** (ISO) y la **Organización de las Naciones Unidas** (ONU) es un hito clave para el desarrollo sostenible y la estandarización a nivel global. Esta alianza busca alinear los estándares internacionales con los Objetivos de Desarrollo Sostenible (ODS) de la **Agenda 2030**, promoviendo la implementación de mejores prácticas en diversas industrias y sectores.

Es necesario explorar la importancia de este acuerdo, sus implicaciones para el sector empresarial y cómo las organizaciones pueden beneficiarse de **herramientas tecnológicas** como el software de ISOTools para implementar de manera efectiva las normativas ISO.

¿En qué consiste el acuerdo entre ISO y la ONU?

El acuerdo formaliza la colaboración estratégica entre ambas organizaciones para enfrentar los principales **retos globales**, como el **cambio climático**, la **seguridad alimentaria**, **la gestión de recursos naturales** y la **responsabilidad social**.

ISO aporta su experiencia en la creación de estándares internacionales, mientras que la ONU proporciona el marco político y los objetivos globales a través de la Agenda 2030. Esta sinergia permite que los **estándares de ISO** sean una guía práctica para que empresas, gobiernos y otras organizaciones contribuyan de manera efectiva al cumplimiento de los ODS.

Principales áreas de colaboración en el acuerdo entre ISO y la ONU

01. **Sostenibilidad y cambio climático:** Normas como la ISO 14001 (gestión ambiental) y la ISO 50001 (eficiencia energética) ayudan a las organizaciones a reducir su impacto ambiental.

02. **Responsabilidad social:** La ISO 26000 promueve prácticas empresariales éticas y responsables.

03. **Innovación y digitalización:** La ISO 56002 fomenta la gestión de la innovación.

04. **Calidad y seguridad:** Estándares como la ISO 9001 (gestión de calidad) y la ISO 45001 (seguridad y salud en el trabajo) son esenciales para mejorar la eficiencia y seguridad empresarial.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Gestión de riesgos de la IA: entender las amenazas asociadas a los sistemas de IA

La **gestión de riesgos de la IA** busca identificar, evaluar, priorizar, eliminar, mitigar o buscar formas para convivir con una amenaza o aprovechar una oportunidad asociadas al uso o desarrollo de sistemas de Inteligencia Artificial. Para ello, acude a una serie de herramientas, principios y marcos normativos como **ISO 42001**.

Repitiendo un axioma reconocido en gestión de riesgos, **lo que se busca es disminuir el peligro y aumentar el beneficio**. Entonces, ¿qué hace diferente la gestión de riesgos de la IA? La respuesta está en lo particular y específico del tipo de riesgo del que se ocupa.

Relación entre gestión de riesgos de la IA y gobernanza de la IA

La **gobernanza de la Inteligencia Artificial** es el **marco conformado por reglas, políticas y estándares** que rigen la investigación, diseño, desarrollo, uso e, incluso, el desecho de

productos o sistemas de IA. Este entramado de normas busca crear una barrera sólida que impida el acceso no permitido, manteniendo a salvo a las personas de cualquier amenaza que pueda representar la IA.

La gestión de riesgos de la IA está dentro de ese marco de gobernanza y forma parte integral de él. El marco lo conforman el escenario y sus normas. La gestión de riesgos es el vigilante que procura que todo esté bajo control.

La gobernanza es un conjunto de normas, prácticas y procedimientos. La gestión de riesgos de la IA es un proceso que busca mantener a salvo de irrupciones y accesos no permitidos a los sistemas de Inteligencia Artificial, pero también **verificar que esos sistemas no vulneren los derechos de las personas** o su integridad.

Por qué es importante la gestión de riesgos de la IA

La IA **es un avance científico de enorme relevancia, pero también despierta recelos**. Esto no ha impedido que irrumpa en casi todos los sectores de la producción, el comercio y los servicios. A pesar de las dudas, la expectativa sobre las oportunidades asociadas a la innovación, eficiencia y productividad hacen que industrias de todo el mundo se rindan ante esta tecnología.

¿Y los temores? ¿Y los riesgos? Por supuesto, son reales, pero también lo son los beneficios. Ese es el papel de la gestión de riesgos de la IA: favorecer un **uso responsable de las tecnologías de IA** y **crear un marco de trabajo seguro sin dejar de aprovechar las oportunidades.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Principales diferencias entre ISO 27001 e ISO 27002

Las **normas ISO 27001 e ISO 27002** son los dos estándares más reconocidos y utilizados en el mundo de la gestión de la seguridad de la información. Ambas forman parte de la familia de normas ISO/IEC 27000, centradas en proteger la información y la gestión de riesgos de las organizaciones. Sin embargo, aunque están muy relacionadas entre sí, cumplen con propósitos diferentes y se complementan mutuamente. En este artículo, vamos explorar las diferencias clave entre las normas ISO 27001 e ISO 27002, y cómo el software ISOTools puede ayudarte a implementar ambas normas de forma eficiente y personalizada.

¿Qué es ISO 27001?

La norma ISO 27001 es una estándar internacional que sienta los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Su principal objetivo es ayudar a las empresas a gestionar y proteger sus activos de información de forma sistemática y eficaz. ISO/IEC 27001 está centrada en **identificar de riesgos, la implementar controles y mejorar de forma continua el SGSI.**

Características clave de ISO 27001

- **Enfoque basado en riesgos**: ISO 27001 requiere que las empresas identifiquen, evalúen y traten los riesgos que tengan relación con la seguridad de la información.

- **Certificación**: se trata de una norma certificable, por lo que las empresas pueden obtener una certificación oficial que demuestra su cumplimiento con ISO 27001.

- **Estructura de alto nivel (HLS)**: sigue la estructura común de las normas ISO, lo que facilita su integración con otros sistemas de gestión, **como ISO 9001, de gestión de calidad, o ISO 14001, de gestión del medio ambiente.**

¿Qué es ISO 27002?

Por su parte, la norma **ISO 27002** es una guía de buenas prácticas para implementar controles de seguridad de la información. A diferencia de la ISO 27001, no se trata de una norma certificable. Es un documento de apoyo que ofrece recomendaciones detalladas acerca de cómo implementar los controles mencionados en el Anexo A de la norma ISO 27001.

Características clave de ISO 27002

- **Enfoque en controles**: ISO 27002 está centrada en proporcionar una guía práctica acerca de cómo implementar y gestionar **controles de seguridad** concretos.

- **No es certificable**: al ser una guía, no está diseñada para ser certificada por las organizaciones, sino para complementar la implementación de la norma ISO 27001.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo utilizar indicadores adelantados para mejorar la seguridad en el lugar de trabajo

Indicadores adelantados o indicadores rezagados. Los equipos de **seguridad y salud en el trabajo** se enfrentan la disyuntiva sobre el tipo de indicadores que utilizarán para desarrollar estrategias enfocadas en un objetivo común: garantizar el bienestar, la integridad y la salud de los trabajadores.

La carencia de automatización que permite disponer de información en tiempo real es motivo de que la gestión SST haya hecho mayor uso de los indicadores rezagados. Los indicadores adelantados buscan **aportar información que permita actuar antes de que un problema aparezca o se agrave**. Sin embargo, la ausencia de apoyo tecnológico provocaba que la información que reportaban no fuera actual y los eventos que se hubiesen podido evitar, tuvieran lugar.

La incursión de la tecnología en la gestión relacionada con salud y seguridad en el trabajo ha permitido que los indicadores adelantados recobren su **poder preventivo y proactivo**.

Qué son indicadores adelantados

Los indicadores adelantados entregan información que **facilita anticiparse a sucesos negativos**. Los rezagados, en contraposición, informan sobre hechos ya cumplidos que han causado problemas y han afectado de forma desfavorable a los trabajadores.

El número de reportes de incidentes sin heridos es un buen ejemplo de indicador adelantado. Este señala que es preciso abordar la **investigación de los incidentes**, establecer la causa raíz, solucionarla y **evitar que este tipo de eventos se conviertan en accidentes con heridos** o consecuencias más lamentables.

El número de heridos en un determinado periodo es un indicador rezagado. Por supuesto, es un indicador sobre el que también hay que trabajar. Pero el hecho principal, los trabajadores heridos, es irreversible.

Ejemplos hay de indicadores adelantados en la gestión de seguridad y salud en el trabajo

La calificación de adelantado se asigna en función de la capacidad que ofrezca la información reportada para actuar y revertir una tendencia o evitar un evento negativo. Los indicadores adelantados **permiten diseñar estrategias proactivas para eliminar riesgos o minimizar el impacto negativo**.

10 formas de celebrar el Día mundial de la energía 2025 con la norma ISO 50001

La energía es un recurso fundamental para el desarrollo de la sociedad y el funcionamiento de las empresas. Sin embargo, su uso ineficiente puede generar impactos negativos tanto en el medio ambiente como en la economía de las organizaciones. Por ello, cada **14 de febrero**, se celebra el **Día Mundial de la Energía**, una fecha clave para concienciar sobre la **importancia del ahorro energético y** la transición hacia **fuentes más sostenibles**.

En este contexto, la **norma ISO 50001** se ha convertido en un estándar de referencia para la implementación de **Sistemas de Gestión de la Energía (SGE)** en las organizaciones. Su adopción permite establecer procesos para **reducir el consumo energético**, optimizar los recursos y minimizar el impacto ambiental, contribuyendo al desarrollo sostenible.

Día mundial de la energía

En 2025, las empresas tienen la oportunidad de celebrar el **Día Mundial de la Energía** aplicando los principios de la **ISO 50001** para mejorar su desempeño energético. A continuación, presentamos **10 formas prácticas para conmemorar esta fecha** e impulsar una cultura organizacional orientada a la eficiencia energética.

1. Realizar una auditoría energética

Una **auditoría energética** es fundamental para identificar áreas de mejora en el consumo de energía. Este proceso implica evaluar el uso actual de la energía y detectar oportunidades para **aumentar la eficiencia**. La ISO 50001 proporciona un marco para llevar a cabo estas **auditorías de manera sistemática**.

2. Establecer una política energética

Desarrollar una **política energética** clara demuestra el compromiso de la organización con la **gestión eficiente de la energía**. Esta política debe alinearse con los objetivos estratégicos y servir como guía para todas las actividades relacionadas con la energía.

3. Definir objetivos y metas energéticas en el Día mundial de la energía

Establecer **objetivos y metas** específicos, medibles, alcanzables, relevantes y con un tiempo definido (SMART) es esencial para **mejorar el desempeño energético**. La ISO 50001 enfatiza la importancia de fijar estas metas para guiar los esfuerzos de la organización.

Claves de la certificación en ISO 27701

La norma **ISO/IEC 27701** surge como una extensión de la **ISO/IEC 27001** para establecer un marco sólido de **gestión de la información de privacidad**. Este estándar ayuda a las empresas a demostrar cumplimiento con regulaciones como el **Reglamento General de Protección de Datos (GDPR)** y otras normativas locales de protección de datos.

En el desarrollo de las siguientes líneas nos centraremos en explorar las claves de la certificación en **ISO 27701**, su impacto en el sector empresarial y cómo un **Software especializado**, como el que ofrece **ISOTools**, facilita su implementación y mantenimiento.

¿Qué es la ISO 27701 y por qué es clave para la privacidad?

La **ISO 27701** establece los requisitos para un **Sistema de Gestión de la Información de Privacidad (PIMS, por sus siglas en inglés)**. Se integra con la ISO 27001 y amplía los controles para abordar específicamente la **gestión de datos personales**, alineando las prácticas organizacionales con los principios de privacidad y seguridad.

Beneficios clave de la certificación

01. **Cumplimiento normativo**: Facilita la alineación con regulaciones de privacidad como el **GDPR**, **CCPA** y otras leyes internacionales.

02. **Confianza y transparencia**: Refuerza la confianza de clientes, socios y empleados en la **protección de sus datos personales**.

03. **Reducción de riesgos**: Minimiza la posibilidad de sanciones y multas por incumplimiento normativo.

04. **Ventaja competitiva**: Diferencia a las organizaciones que demuestran un compromiso real con la privacidad.

05. **Optimización de procesos**: Mejora la eficiencia en la gestión de la seguridad de la información y la privacidad.

Claves para la certificación en ISO 27701

1. Integración con la ISO 27001

Para obtener la certificación en ISO 27701, es indispensable contar previamente con un **Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001**. La nueva norma amplía este marco incluyendo requisitos específicos de privacidad.

2. Identificación de roles: Responsables y encargados del tratamiento, la ISO 27701 diferencia entre:

- **Responsables del tratamiento**: Organizaciones que recopilan y deciden el propósito de los datos personales.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Gestión del cumplimiento de la IA con la norma ISO 42001

La gestión del **cumplimiento de la IA** entra en una nueva era con la publicación de la **norma ISO 42001**. Ante la incursión arrolladora de la Inteligencia Artificial en todos los ámbitos de la sociedad y de la producción, era urgente disponer de un estándar confiable y eficaz para la gestión de los sistemas de Inteligencia Artificial.

Esa necesidad fue la principal razón para que, en diciembre de 2023, la Organización Internacional de Estandarización publicara **la primera norma para la gestión del cumplimiento de la IA: ISO 42001**, en colaboración con la Comisión Electrotécnica Internacional (IEC).

El objetivo principal de la norma es **eliminar o mitigar los riesgos asociados al desarrollo o uso de sistemas de Inteligencia Artificial**: igualdad, privacidad de los datos, respeto por los derechos humanos, propiedad intelectual, aprendizaje no supervisado de la IA, etc.

Componentes de la gestión del cumplimiento de la IA

La **estructura de ISO 42001 es una estructura de Alto Nivel**, la misma que caracteriza a otros estándares tan conocidos como ISO 9001, ISO 45001 o ISO 14001, lo que facilitará la integración en el futuro. El estándar incorpora tres componentes clave:

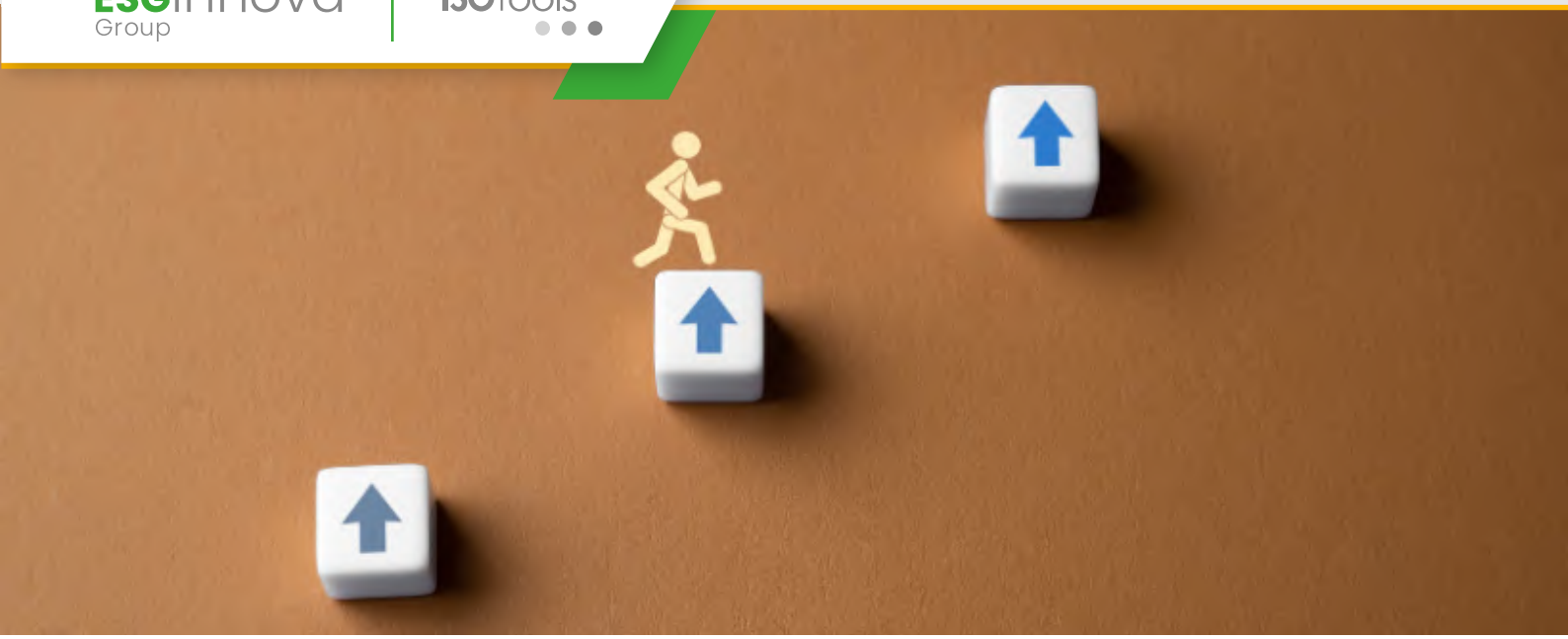
- **Gobernanza ética**: directrices diseñadas para asegurar el desarrollo y uso ético de los sistemas de IA. Es el componente que se encarga del uso responsable y transparente de la IA.

- **Transparencia y rendición de cuentas**: requisitos que buscan que las organizaciones implementen procesos que permitan obtener respuestas a inquietudes de usuarios u otras partes interesadas, generando así confianza y credibilidad.

- **Gestión de riesgos**: las organizaciones diseñarán e implementarán procesos eficaces de **gestión de riesgos de la IA** específicos del uso o desarrollo de sistemas de Inteligencia Artificial.

Quiénes deben asegurar la gestión del cumplimiento de la IA en ISO 42001

ISO 42001 no es un estándar obligatorio, pero tampoco reservado. **Lo pueden aplicar todo tipo de organizaciones**, de todos los tamaños, todas las complejidades y sin considerar la ubicación o el sector en el que opera. Sin embargo, dado el objetivo tan específico de la norma, no es productivo que una empresa que no desarrolla ni hace uso de sistemas de Inteligencia Artificial la implemente.



Todo lo que vale la pena conocer acerca de la norma ISO 22301

Los desastres naturales, fallos tecnológicos o crisis inesperadas, constituyen un desafío para la continuidad de negocio, en este sentido, la capacidad de una organización para recuperarse y seguir operando es vital para su supervivencia y éxito. Es en este contexto la **Norma ISO 22301** es una herramienta muy valiosa.

En este artículo, se explora todo lo que necesitas saber sobre la ISO 22301 norma, su definición, beneficios, su implementación, y cómo herramientas como **ISOTools** pueden simplificar y optimizar este proceso.

¿Qué es la Norma ISO 22301?

La **ISO 22301** es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora de un **Sistema de Gestión de Continuidad del Negocio (SGCN)**. Su primera publicación fue en 2012 y se actualizó en 2019.

Esta norma establece un marco estructurado para que las organizaciones identifiquen amenazas potenciales, evalúen su impacto y desarrollen planes para garantizar la continuidad de sus operaciones críticas.

El objetivo principal de la norma ISO 22301 es ayudar a las empresas a **prepararse, responder y recuperarse de forma eficiente ante incidentes, y minimizar así el impacto en sus operaciones, reputación y relaciones con los clientes.**

Beneficios de implementar ISO 22301

Implementar la **Norma ISO 22301** tiene muchos **beneficios para las empresas**, independientemente de su tamaño o sector. Algunos de los más destacados son los siguientes:

Resiliencia empresarial

ISO 22301 permite a las organizaciones a ser más resistentes ante interrupciones, lo que les permite **mantener sus operaciones críticas** incluso en situaciones adversas o inesperadas.

Protección de la reputación

Una respuesta rápida y efectiva ante crisis **protege la imagen de la empresa y fortalece la confianza** de los clientes y partes interesadas.

Cumplimiento legal

Muchas industrias exigen planes de continuidad del negocio como parte de sus requisitos legales.

¿Qué son los CTN o Comités Técnicos de Normalización de normas ISO?

La **normalización** es un proceso fundamental para garantizar la calidad, seguridad y eficiencia de productos, servicios y sistemas en todo el mundo. Dentro de este marco, los **Comités Técnicos de Normalización (CTN)** desempeñan un papel clave en el desarrollo y revisión de normas internacionales, incluyendo las de la **Organización Internacional de Normalización (ISO)**.

Los **CTN** reúnen a expertos de distintos sectores para elaborar estándares que favorezcan la **competitividad** y el **cumplimiento de requisitos técnicos**. Pero, ¿qué son exactamente los CTN y cómo influyen en la creación de normas ISO? En este artículo, analizamos su función, estructura y relevancia en el ámbito de la normalización.

CTN

Un **Comité Técnico de Normalización (CTN)** es un grupo de trabajo conformado por expertos de diferentes sectores industriales,

académicos y gubernamentales con el objetivo de **desarrollar, revisar y actualizar normas técnicas**. Estos comités trabajan bajo el amparo de organismos nacionales e internacionales de normalización.

Funciones principales de los CTN

Los **CTN** tienen varias **responsabilidades** clave en la creación de normas ISO, entre las que destacan:

- **Elaboración de nuevas normas**: Desarrollan estándares que regulan aspectos técnicos y de gestión en diversos sectores.
- **Revisión y actualización**: Evalúan periódicamente las normas existentes para asegurar que siguen siendo relevantes y efectivas.
- **Participación en el desarrollo de normas ISO**: Colaboran con la **Organización Internacional de Normalización (ISO)** en la redacción y mejora de estándares globales.
- **Recepción y análisis de propuestas**: Consideran sugerencias de la industria y otros organismos para mejorar la normalización.
- **Promoción de la armonización normativa**: Buscan la alineación de normas nacionales con estándares internacionales para facilitar el comercio y la interoperabilidad.

Estructura y organización de los CTN

Los **CTN** están organizados en **diferentes niveles** y trabajan bajo la coordinación de organismos nacionales e internacionales.

¿Qué es ISO 27032 Directrices para la ciberseguridad?

La conectividad y la dependencia de las tecnologías son fundamentales para el funcionamiento de las empresas. Por tanto, la **ciberseguridad** se ha convertido en una necesidad esencial para proteger tanto los activos de la organización como la privacidad de los usuarios.

Ante este contexto, la **norma ISO 27032**, conocida como **«Directrices para la Ciberseguridad»**, se presenta como una herramienta clave para las organizaciones que desean fortalecer su infraestructura de seguridad y mitigar los riesgos asociados con las amenazas cibernéticas.

¿Qué es ISO 27032?

ISO 27032 es un **estándar internacional que ofrece directrices detalladas sobre la gestión de la ciberseguridad**, especialmente en el contexto de la **seguridad de la información**.

A pesar de que forma parte de la familia de normas ISO/IEC 27000, que abordan la gestión de la seguridad de la información, ISO 27032 se centra exclusivamente en las **amenazas y riesgos asociados con el ciberespacio**. Su principal objetivo es proporcionar un marco para ayudar a las organizaciones a implementar medidas eficaces contra los riesgos cibernéticos y proteger la confidencialidad, integridad y disponibilidad de los sistemas digitales.

La norma no se limita solo a la protección interna de las organizaciones, sino que también promueve la **colaboración con otras partes interesadas**, como gobiernos, empresas y usuarios, para crear un **entorno digital más seguro**.

¿Qué cubre ISO 27032?

La norma ISO 27032 cubre diversas áreas esenciales para gestionar la ciberseguridad de manera efectiva. A continuación, destacamos algunos de los puntos clave que abarca:

01. Protección de Infraestructuras Críticas

Una de las principales preocupaciones de ISO 27032 es garantizar la protección de infraestructuras críticas en las organizaciones, tales como redes, sistemas de comunicación, bases de datos y plataformas en la nube. Los ataques cibernéticos dirigidos a estas infraestructuras pueden tener consecuencias devastadoras, por lo que esta norma ofrece directrices para reforzar su seguridad.

02. Gestión de Vulnerabilidades

La norma también hace hincapié en la importancia de gestionar las vulnerabilidades de los sistemas tecnológicos.

Por qué es necesario comprender la ISO 27017

En la era digital, la **seguridad en la nube** se ha convertido en una preocupación clave para empresas y organizaciones que **almacenan y gestionan información** en entornos virtuales. La creciente adopción de servicios en la nube ha generado la necesidad de contar con estándares específicos que garanticen la **protección de los datos**. Es aquí donde entra en juego la **ISO 27017**, una norma internacional que proporciona directrices para **mejorar la seguridad en la nube**, complementando el marco de **ISO 27001** sobre **gestión de seguridad de la información**.

Comprender la **ISO 27017** es fundamental para las empresas que utilizan o proporcionan servicios en la nube, ya que ayuda a mitigar riesgos y garantizar la **confidencialidad, integridad y disponibilidad** de la información. En este artículo, exploraremos en detalle qué es la **ISO 27017**, sus beneficios, los controles específicos que introduce y su relación con otras normas de seguridad.

ISO 27017

La **ISO 27017** es un estándar internacional que proporciona **controles adicionales de seguridad para servicios en la nube**. Fue desarrollado por la **Organización Internacional de Normalización (ISO)** como una extensión de la **ISO 27001**, con el objetivo de abordar riesgos específicos asociados a la computación en la nube.

Características principales de la ISO 27017

- Proporciona **directrices específicas** para proveedores y clientes de servicios en la nube.
- Se basa en la estructura de la **ISO 27002**, con controles adicionales para entornos cloud.
- Ayuda a mitigar riesgos como la **pérdida de datos, accesos no autorizados y vulnerabilidades en la infraestructura**.
- Facilita el **cumplimiento de requisitos legales y regulatorios** relacionados con la seguridad en la nube.

Beneficios de implementar la ISO 27017

Implementar la **ISO 27017** no solo refuerza la seguridad de la información, sino que también brinda **ventajas competitivas** a las empresas que la adoptan.

Mejora la seguridad en entornos cloud

Este estándar proporciona controles específicos para **identificar y gestionar los riesgos asociados a la computación en la nube.**

ESGinnova
Group

HSE Tools

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

Cumplimiento normativo de HSE: 5 formas de simplificarlo con software

Garantizar el cumplimiento normativo de HSE es uno de los desafíos más complejos en el acontecer corporativo de una organización. La volatilidad de los **requisitos legales**, de un marco regulatorio dominado por estándares, leyes y directivas de alcance internacional algunas de ellas, es el primer factor que agrega complejidad a la tarea.

La necesidad de **recopilar, procesar y analizar grandes cantidades de datos** y la expansión de las cadenas de suministro hacia los cuatro puntos cardinales del planeta completan un escenario en el que es cada día más complejo garantizar el cumplimiento normativo de HSE. **Supervisión, agilidad y capacidad de adaptación son las claves**. Sin estos tres elementos, el cumplimiento normativo de HSE puede convertirse en un obstáculo difícil de salvar, generando dificultades para operar, costes inesperados, sanciones y afectación a la reputación, entre otras consecuencias.

Consecuencias de ignorar el cumplimiento normativo de HSE

Las consecuencias, como ya se adelanta, son serias. Estas incluyen **impacto financiero, deterioro de la reputación, litigios judiciales** y, a largo plazo, perdida de confianza de los consumidores e inversionistas. El impacto negativo en áreas específicas como **Gestión Ambiental** o Seguridad y Salud en el Trabajo es también considerable, desde contaminación de fuentes de recursos naturales hasta incremento de accidentes. No trabajar para asegurar el cumplimiento normativo de HSE puede, incluso, **paralizar las operaciones como consecuencia de la aplicación de cierres sucesivos de la actividad o de la pérdida de licencias**. Sanciones y tiempo de inactividad deterioran la confianza de los trabajadores, de los clientes, de los inversionistas y de los organismos reguladores, entre otras partes interesadas. Más allá de la preocupación por los bienes de la empresa y por sus finanzas está **el bienestar de las personas: empleados, comunidad, consumidores, etc.** La protección y el bienestar de todas las personas expuestas al impacto de la operación de la empresa tiene que ser la principal razón para velar por el cumplimiento normativo de HSE.

Cómo simplificar los procesos de cumplimiento normativo de HSE aprovechando la tecnología

Garantizar el cumplimiento normativo de HSE parece, a la luz de lo expuesto, una tarea ardua. Lo es cuando se trabaja con procesos basados en documentos e informes en papel. Incluso la gestión basada en hojas de cálculo es dispendiosa y proclive al error humano. La solución pasa por **utilizar una herramienta tecnológica que tenga entre sus funcionalidades el cumplimiento legal y normativo**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Guía completa para implementar una matriz de riesgos

Una de las herramientas más efectivas para identificar, evaluar y gestionar los conflictos que puedan surgir en el entorno empresarial es la matriz de riesgos, una herramienta visual que permite priorizar las amenazas y oportunidades dentro de la organización.

A continuación, te proporcionaremos una guía completa sobre cómo implementar una **matriz de riesgos**, con un enfoque especial en cómo las empresas pueden mejorar su gestión de riesgos mediante el uso de un **Software de Gestión de Riesgos**, como el que ofrece **HSETools**.

¿Qué es una matriz de riesgos?

Una **matriz de riesgos** es una herramienta que permite evaluar y priorizar los riesgos de una organización en función de dos variables principales: la **probabilidad** de que ocurra un evento de riesgo y

el **impacto** que tendría en caso de suceder. Esta matriz se presenta comúnmente como una tabla, donde se asignan puntuaciones a cada riesgo según su probabilidad e impacto, lo que facilita la toma de decisiones para mitigar o gestionar dichos riesgos.

Pasos para implementar una matriz de riesgos

Definición de riesgos

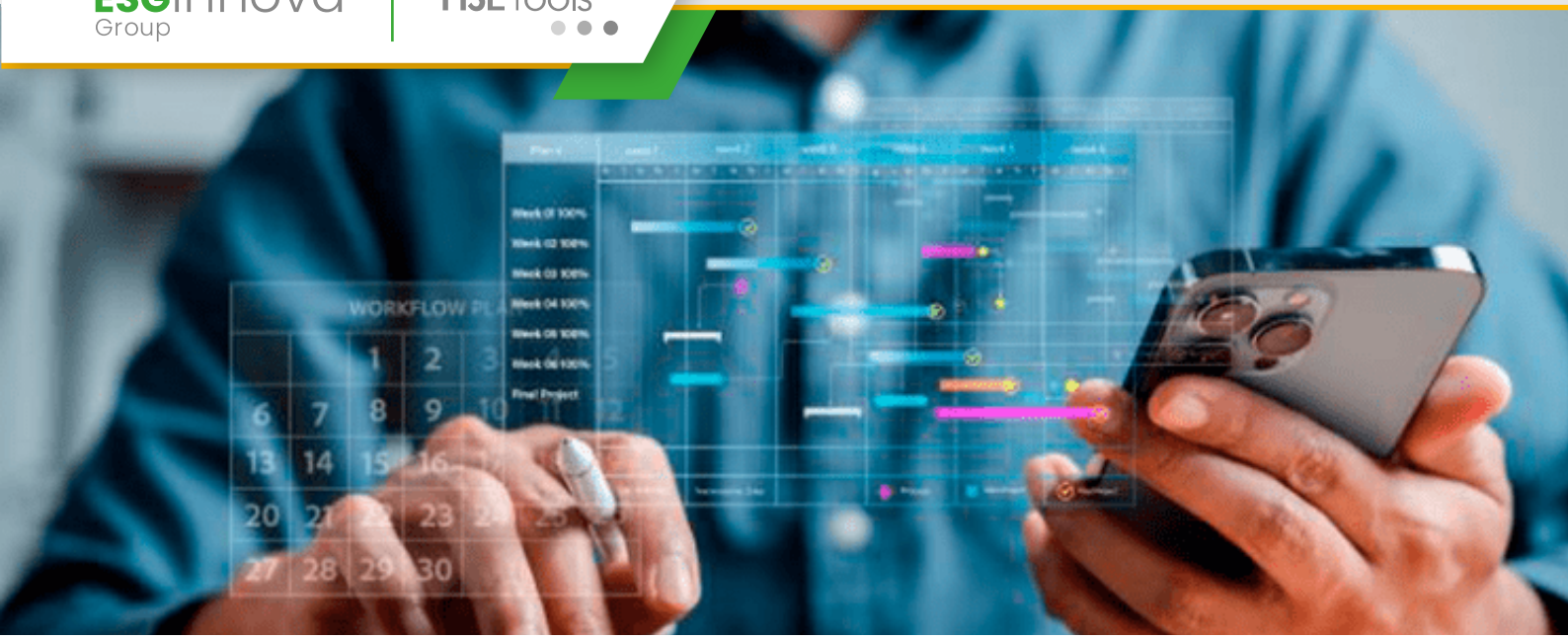
El primer paso en la implementación de una matriz de riesgos es **identificar todos los riesgos potenciales** que puedan afectar a la organización. Estos pueden clasificarse en riesgos internos (como fallas en procesos o errores humanos) y riesgos externos (como cambios regulatorios o desastres naturales). La identificación debe ser exhaustiva, involucrando a diferentes áreas de la empresa, como operaciones, recursos humanos, IT y salud y **seguridad laboral**.

Evaluación de la probabilidad y el impacto

Una vez identificados los riesgos, se debe evaluar tanto la probabilidad de que ocurran como el impacto que tendrían. Es importante asignar una **escala numérica o categórica** (por ejemplo, bajo, medio o alto) para clasificar estos dos factores. A través de esta evaluación, podrás visualizar cuáles son los riesgos más significativos para la organización.

Construcción de la matriz

La matriz se crea cruzando las **categorías de probabilidad** con las **categorías de impacto**. Esto da como resultado una cuadrícula donde los riesgos se ubican en función de su evaluación.



Por qué debería automatizar los flujos de trabajo de gestión de contratistas

La automatización de flujos de trabajo de gestión de contratistas es, tal vez, la funcionalidad que mayor atracción genera en los responsables de seguridad y salud en el trabajo que buscan la aprobación de la Alta Dirección para un proyecto de digitalización basado en un software especializado.

La transformación digital avanza imparable en el mundo corporativo y la gestión de contratistas no es ajena a la tendencia. La tecnología tiene el poder de **cambiar la forma en que contratistas y empresas abordan temas legales, comerciales, estructurales y prácticos** involucrados en esta modalidad de contratación de fuerza laboral.

Gestión de contratistas y tecnología

En los flujos de trabajo de gestión de contratistas se involucran **temas como seguridad, competencias, documentos legales, productividad**, tarifas, uso de **equipos de protección personal** y otros que demandan tiempo y recursos para su adecuada gestión. Las oportunidades que encuentran las empresas al obtener la colaboración de contratistas justifican la tendencia creciente hacia el uso de terceros. La complejidad de los flujos de trabajo de gestión de contratistas es la razón principal por la que fabricantes y proveedores de software resaltan **la capacidad de automatización de la gestión cómo su más alto valor.** Automatizar los flujos de trabajo de gestión de contratistas **ahorra tiempo y dinero a las empresas** y permite generar relaciones cordiales y productivas con los trabajadores bajo esta modalidad. El proyecto de automatización, sin embargo, requiere el aval de la Alta Dirección.

Razones para automatizar los flujos de trabajo de gestión de contratistas

Si se examina en detalle, **el proceso que va desde la selección de un contratista hasta el cierre del contrato implica cientos de tareas**. Son tantas y tan complejas, que pueden resultar abrumadoras. Eliminar tareas o procesos de los flujos de trabajo de gestión de contratistas no es la solución. Las actividades, los procesos y las tareas están ahí por una razón y es cierto que demandan tiempo, dinero y recursos. Pero, ¿necesariamente esto tiene que ser así? La respuesta es no, pero el consumo desbordado de tiempo, dinero y recursos tampoco es obligatorio. **La respuesta está en la automatización.**

ROI de un software HSE: aspectos cualitativos y cuantitativos que justifican la inversión

El ROI de un software HSE es evidente, comprobable y rápido. Esta frase contundente responde a la inquietud de muchos profesionales que evalúan la posibilidad de automatizar la **gestión HSE** en sus respectivas organizaciones y se enfrentan a la tarea de convencer a la Alta Dirección sobre los beneficios del proyecto.

La automatización de la gestión de seguridad y salud en el trabajo y ambiental evita multas y sanciones. No es el único argumento para explicar el ROI de un software HSE. Las formas en que la **inversión en un software HSE** amortiza su coste son varias. Para entenderlo, es preciso evaluar aspectos cualitativos y cuantitativos que es necesario exponer ante la Alta Dirección para justificar la inversión. En el proceso de desglosar y entender las diferentes formas en que se presenta el ROI de un software HSE, las organizaciones, los equipos dedicados y la misma Alta Dirección

pueden observar que **existen herramientas y funcionalidades que tienen capacidad de potenciar aún más el retorno de la inversión**.

Cómo se genera el ROI de un software HSE

El ROI de un software HSE aparece en el inmediato, el medio y el largo plazo. Algunas manifestaciones del retorno de la inversión requieren de una evaluación cualitativa y otras se muestran en cifras concretas.

1. ROI de un software HSE de carácter inmediato

La recuperación de la inversión generada por los efectos positivos del software puede aparecer en periodos de tiempo que **no superan los seis meses iniciales del proyecto:**

- **Disminuye o elimina incidentes, casi accidentes y accidentes**: su impacto sobre las finanzas es claro, ya que se reducen costes médicos, **absentismo laboral** y costes judiciales o compensatorios. Estos pueden afectar seriamente a las finanzas de empresas que no cuentan con un sistema de gestión HSE automatizado y eficiente que entregue información en tiempo real, promoviendo la acción inmediata y proactiva.

- **Reduce el consumo de horas de trabajo**: la gestión ineficaz demanda más horas de trabajo que la gestión efectiva. Esta aprovecha la digitalización, acudiendo a tecnologías como Big Data e Inteligencia Artificial.

- **Acceso inmediato a información centralizada**: el software entrega información completa en tiempo real.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué define el Decreto 1072 de 2015 que debe incluir la inducción en SST?

La seguridad y salud en el trabajo (SST) es una prioridad en cualquier organización comprometida con el bienestar de sus colaboradores y el cumplimiento normativo. En Colombia, el Decreto 1072 de 2015 establece lineamientos claros sobre la implementación del **Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST)**, incluyendo la inducción y capacitación de los trabajadores en materia de prevención de **riesgos laborales**.

Es necesario tratar en profundidad **qué establece el Decreto 1072 de 2015** sobre la inducción en SST, y cómo las empresas pueden mejorar su gestión a través de herramientas tecnológicas como HSETools.

¿Qué establece el Decreto 1072 de 2015 sobre la inducción en SST?

El **Decreto 1072 de 2015** es un compendio normativo que reglamenta el SG-SST en **Colombia**. En lo que respecta a la inducción en seguridad y salud en el trabajo, exige que todas las empresas, sin importar su tamaño o sector, brinden capacitaciones a sus empleados, contratistas y personal nuevo para garantizar el conocimiento de los riesgos y medidas preventivas en su lugar de trabajo.

Elementos clave de la inducción en SST según el Decreto 1072 de 2015

El decreto estipula que la inducción en SST debe incluir los siguientes aspectos:

01. **Política del SG-SST**: La empresa debe comunicar su compromiso con la seguridad y salud en el trabajo.

02. **Identificación de peligros y evaluación de riesgos**: Explicar los riesgos específicos del cargo y las medidas de prevención.

03. **Normas y procedimientos de seguridad**: Instrucciones sobre el uso de equipos de protección personal (EPP), señalización, higiene y buenas prácticas laborales.

04. **Actuación en emergencias**: Protocolos para evacuaciones, incendios, primeros auxilios y otras situaciones de riesgo.

05. **Derechos y deberes de los trabajadores en SST**: Responsabilidades en la prevención de accidentes y enfermedades laborales.

Cómo realizar evaluaciones de desempeño de contratistas: factores a tener en cuenta

Las evaluaciones de desempeño de contratistas implican mucho más que la calificación del resultado final del trabajo encomendado o el proyecto asignado. Más allá de un trámite burocrático, constituyen una de las claves de una óptima **gestión de contratistas**, puesto que ofrecen una información de gran valor.

Lo cierto es que **el rendimiento adecuado en un proyecto en el que se cuente con la colaboración de terceros depende de muchos factores**: capacitación, documentos, capacidad técnica y operativa para realizar el trabajo, respeto por las normas de seguridad o cumplimiento del cronograma de avance son algunos de los más relevantes. Las evaluaciones de desempeño de contratistas entregan información sobre el desempeño del contratista de acuerdo con esos factores. Esa información es muy valiosa para **tomar decisiones oportunas y bien fundamentadas**, que corrijan el rumbo cuando así lo indiquen los resultados o permitan potenciar y mejorar aún más los resultados, cuando ese sea el caso.

Factores que se revisan en las evaluaciones de desempeño de contratistas

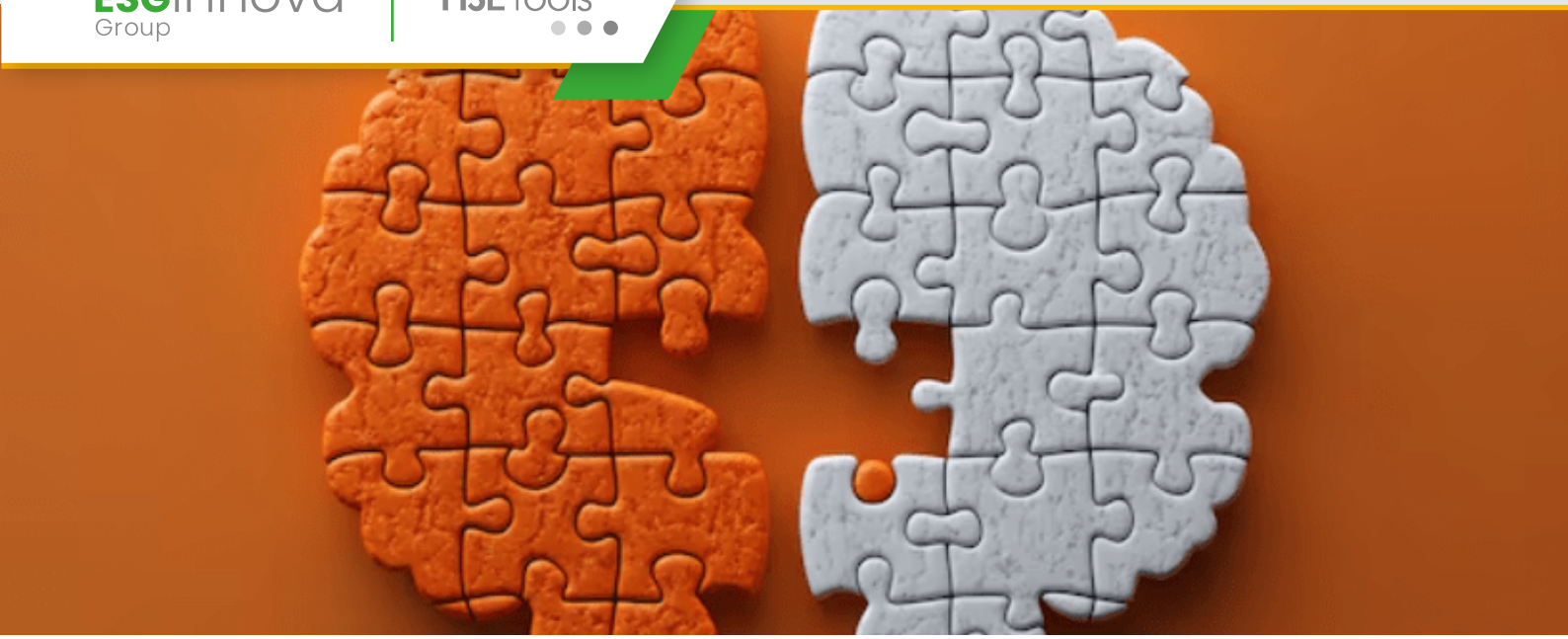
Los resultados de las evaluaciones de desempeño de contratistas **sirven para planificar el trabajo hacia el futuro, identificar riesgos y tomar decisiones informadas** que tendrán impacto positivo sobre el bienestar de los trabajadores, sobre el desarrollo esperado del proyecto y sobre la estrategia comercial de la organización. Para que las evaluaciones de desempeño de contratistas entreguen los resultados esperados, **es necesario saber qué buscar, qué revisar y qué evaluar**. La siguiente lista de verificación, sumada al uso de una solución tecnológica para **automatizar los flujos de trabajo de gestión de contratistas**, será suficiente para obtener el máximo provecho de la evaluación:

1. Documentación requerida

El **control de documentación de contratistas** permite **establecer el cumplimiento de los requisitos formales, de formación y capacitación y de documentación** solicitados por la organización de acuerdo con el perfil requerido. Así, en evaluaciones de desempeño de contratistas, las siguientes cuestiones son fundamentales:

- ¿El contratista puede entregar **documentos para acreditar su experiencia**?
- ¿Cuenta con las **certificaciones de programas de formación mínimos**, como trabajo en alturas, manipulación de alimentos, prevención de riesgos u otros requeridos para la ejecución de la tarea?

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Cómo se construye un arbol de problemas?

En la gestión de proyectos, la planificación estratégica y el análisis de riesgos, el arbol de problemas es una herramienta clave para identificar y comprender las causas y efectos de un problema dentro de una organización. Esta metodología permite estructurar visualmente los factores que influyen en un problema central, facilitando la toma de decisiones y el diseño de soluciones efectivas.

El **arbol de problemas** se usa ampliamente en entornos de **Salud, Seguridad y Medioambiente (HSE)**, gestión de riesgos y planificación empresarial. Su aplicación permite a las organizaciones **abordar incidentes, reducir accidentes laborales y mejorar el cumplimiento normativo**.

En este artículo, exploraremos cómo construir un **arbol de problemas**, sus elementos principales y los beneficios de su aplicación en distintos sectores.

Arbol de problemas

El **arbol de problemas** es una representación gráfica que ayuda a **identificar, analizar y estructurar** los factores que contribuyen a una determinada problemática. Se basa en una relación causa-efecto, donde el problema central actúa como el **tronco**, las causas como las **raíces** y los efectos como las **ramas**.

Elementos clave de un arbol de problemas

- **Problema central:** la situación o dificultad que se quiere analizar y resolver.
- **Causas primarias y secundarias:** los factores que originan el problema y que pueden clasificarse en causas directas e indirectas.
- **Efectos o consecuencias:** las repercusiones derivadas del problema central en la organización o el entorno.

Pasos para construir un arbol de problemas

1. Definir el problema central

El primer paso es identificar claramente el problema a analizar. Para ello, se recomienda **formularlo en términos específicos y objetivos**, evitando generalizaciones.

Ejemplo: En una empresa del sector industrial, un problema recurrente puede ser **«alto índice de accidentes laborales»**.

Los 5 principales riesgos de gestionar procesos de gestión de la seguridad laboral de forma manual

Los procesos de gestión de la seguridad laboral desarrollados en papel, o en algunos casos asistidos por hojas de cálculo, presentan fisuras y brechas que permiten la proliferación de riesgos. Al contrario, la tecnología provee las herramientas suficientes para garantizar una eficiente **gestión de documentos y registros**, esencial para enfrentarse a las amenazas y evitar incumplimientos.

La exposición al error humano, el consumo desmesurado de horas de trabajo o la imposibilidad para obtener trazabilidad de la información y de los documentos son dificultades que presenta la gestión manual. Por eso, **la reducción de costes relacionados con la seguridad depende en buena medida de la automatización** de los procesos de gestión de la seguridad laboral.

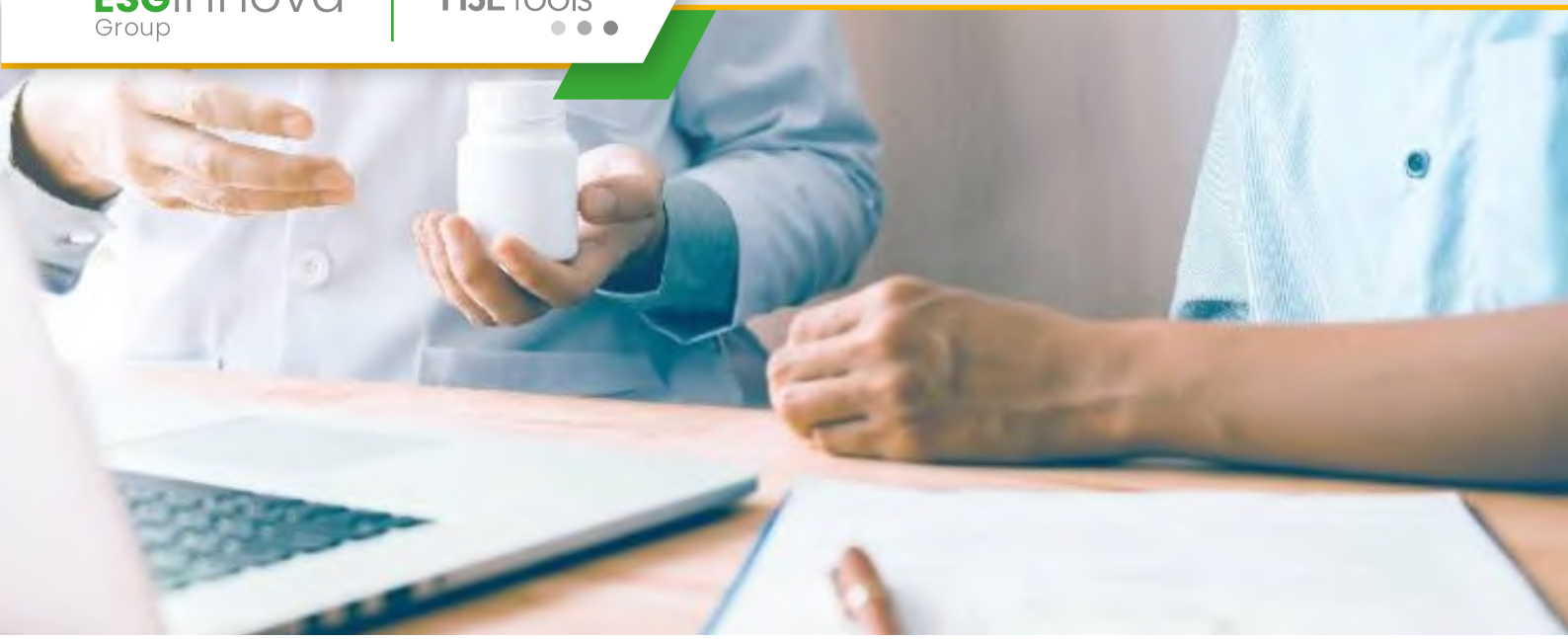
Riesgos de los procesos de gestión de la seguridad laboral que se realizan de forma manual

La principal motivación para contar con procesos de gestión de la seguridad laboral es, por supuesto, garantizar la integridad y el bienestar de las personas. Es la principal, pero no la única. **Cumplir con leyes, decretos, normativas o regulaciones es también un objetivo válido y relevante**. Mejorar la percepción como empleador, aportar valor a la marca, **mejorar la reputación corporativa** o cumplir requisitos exigidos en algunos mercados también justifican invertir en la seguridad en el trabajo. Pero lo más importante es **entender que hay un buen número de riesgos que se pueden evitar** automatizando los procesos de gestión de la seguridad laboral.

1. Exceso de trabajo, costes y recursos en general

En un escenario teórico, se presenta un incidente que causó lesiones a varios trabajadores en un lugar remoto. Los equipos de seguridad se desplazan hasta él para recopilar la información que les permita investigar la causa raíz, evaluar los riesgos y proponer acciones correctivas.

El proceso de implementación de una acción correctiva, verificada y comprobada, puede llevar semanas. En una gestión manual hay una inversión considerable en horas de trabajo y recursos, además, se generan decenas de documentos que es necesario almacenar y que no siempre son accesibles o se pueden compartir. De esta forma, **no es posible afrontar una gestión de riesgos proactiva**.



5 actividades clave para mejorar la salud ocupacional de la empresa

Pasamos en torno al 40% de nuestra vida trabajando, por lo que crear un entorno de trabajo seguro y saludable es vital para **mejorar la calidad de vida de todos**. Esto a su vez es sinónimo de productividad, lo que da lugar a una reducción de costos asociados a bajas laborales, accidentes y enfermedades profesionales a través de la **Vigilancia de la Salud**.

Las empresas que apuestan por la salud y seguridad de sus colaboradores tienen mayores índices de satisfacción laboral y compromiso organizacional. Pero, ¿cómo pueden las organizaciones mejorar en este aspecto? Aquí te presentamos **cinco actividades clave** para fortalecer la salud ocupacional en tu empresa.

1. Evaluación y gestión de riesgos laborales

El primer paso para garantizar la salud ocupacional es realizar una evaluación exhaustiva de los **riesgos presentes en el lugar**

de trabajo. Factores como ergonomía, exposición a sustancias peligrosas, estrés laboral o condiciones ambientales pueden afectar la salud de los trabajadores. Para ello, es fundamental:

- Identificar los peligros asociados a cada puesto de trabajo.
- Evaluar los riesgos y su nivel de criticidad.
- Implementar medidas de control y prevención.
- Realizar auditorías periódicas para actualizar la evaluación de riesgos.
- Una adecuada gestión de los riesgos permite **reducir la siniestralidad laboral** y crear ambientes de trabajo más seguros y saludables.

2. Implementación de programas de promoción de la salud

No basta con evitar riesgos; las empresas deben fomentar el bienestar de sus empleados a través de programas de promoción de la salud. Algunas acciones recomendadas incluyen:

- **Pausas activas** para reducir el sedentarismo y mejorar la circulación.
- **Charlas sobre alimentación saludable** y bienestar físico.
- **Fomento de la actividad física** mediante convenios con gimnasios o programas internos.
- **Terapias de reducción del estrés**, como yoga o mindfulness.

Software para Control de Contratistas: 5 señales de que lo necesitas

La inversión en un **Software para Control de Contratistas** siempre es una buena estrategia. Una adecuada **gestión de la fuerza laboral externa** es, además, un proyecto que genera un retorno de la inversión rápido e interesante.

La seguridad de trabajadores y terceros debe ser una prioridad para las empresas. Es una de las razones principales para implementar un Software para Control de Contratistas. Pero, además del cumplimiento en el área SST, también contribuyen al cumplimiento del contrato, de los requisitos legales y contractuales e, incluso, a la elección del perfil de contratista ideal de acuerdo con sus competencias y capacitación. Cumplir siempre será importante. Monitorear y revisar el trabajo de los contratistas desde varios ángulos también lo será. Por esto, un Software para Control de Contratistas será una buena elección en todo momento. Sin embargo, hay **señales que indican que la automatización de la gestión se ha convertido en una necesidad imperiosa**.

Señales que indican que la empresa necesita un Software para Control de Contratistas

El Software para Control de Contratistas gestiona, verifica, evalúa y, resumiendo, controla el trabajo de los trabajadores externos de la organización. Pero esto no significa que solo sirva a la organización, es **una herramienta que aporta beneficios tanto a la empresa como a los contratistas**. Esta solución **genera relaciones de trabajo seguras, transparentes, confiables y productivas**. Solo por eso, trabajar con un Software para Control de Contratistas tendría que ser una decisión que no necesitaría más argumentos. Sin embargo, hay indicios que indican que su utilización no se puede demorar:

1. La gestión de contratistas demanda demasiadas horas de trabajo

Las tareas y las responsabilidades asociadas a la gestión de contratistas son muchas: verificar el cumplimiento de los formalismos documentales, comprobar el avance del trabajo contratado, la supervisión del uso adecuado de **elementos de protección personal** o el respeto por las normas internas de la empresa, entre otras. Cuando el número de contratistas crece, **su gestión puede convertirse en una tarea muy compleja**. Empresas grandes podrían resolver el problema creando un departamento de Gestión de Contratistas. Sin embargo, los costes asociados que esto implica podrían hacer inviable el proyecto en términos financieros. **Un Software para Control de Contratistas automatiza muchas de las tareas** asociadas con la gestión de terceros y con su seguridad, además del cumplimiento de las obligaciones económicas de la organización.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Guía completa acerca de las Charlas de seguridad de 5 minutos

Las **Charlas de seguridad de 5 minutos** son una estrategia efectiva para reforzar la cultura de seguridad en el trabajo. Su objetivo principal es **concienciar a los trabajadores sobre los riesgos laborales** y proporcionar información clave sobre **medidas preventivas** de manera breve y directa.

Estas charlas son ampliamente utilizadas en sectores como la **construcción, manufactura, minería y logística**, donde los riesgos laborales son elevados. Sin embargo, cualquier empresa que busque mejorar su sistema de **Salud, Seguridad y Medioambiente (HSE)** puede implementarlas con éxito.

En esta guía, exploraremos qué son las **Charlas de seguridad de 5 minutos**, cómo implementarlas eficazmente y cuáles son sus beneficios para las organizaciones.

Charlas de seguridad de 5 minutos

Las **Charlas de seguridad de 5 minutos** son reuniones breves que se llevan a cabo antes del inicio de la jornada laboral o antes de realizar una tarea específica. Su propósito es **reforzar conocimientos en seguridad, actualizar a los trabajadores sobre procedimientos y minimizar el riesgo de accidentes**.

Se caracterizan por:

- **Duración corta**, generalmente de 5 a 10 minutos.
- **Enfoque práctico**, con información clara y aplicable al puesto de trabajo.
- **Interactividad**, fomentando la participación de los trabajadores.
- Estas charlas no reemplazan la capacitación formal en seguridad, pero sí refuerzan su aplicación en el día a día.

Beneficios de implementar Charlas de seguridad de 5 minutos

- **Reducción de accidentes laborales:** Mantener la seguridad presente en la mente de los trabajadores ayuda a **identificar y prevenir riesgos** antes de que ocurran incidentes.
- **Mejora del cumplimiento normativo:** Las empresas que llevan a cabo estas charlas regularmente pueden demostrar su **compromiso con la seguridad** y el cumplimiento de normativas como la **ISO 45001** o regulaciones locales de seguridad laboral.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Introducción a la charla de 5 minutos para empresas

La **charla de 5 minutos** es una herramienta efectiva y sencilla que las empresas pueden implementar para reforzar la cultura de **Seguridad y Salud en el Trabajo (SST)** y el cuidado del **Medio Ambiente**. Se trata de una estrategia breve y focalizada que permite transmitir información relevante a los trabajadores en su jornada laboral. A pesar de su corta duración, su impacto puede ser significativo en la prevención de accidentes, el cumplimiento normativo y la **mejora del ambiente laboral**.

A continuación, exploraremos cómo la charla de 5 minutos puede marcar la diferencia en una organización y de qué manera la **implementación del Software de Gestión de Riesgos de HSETools** optimiza este proceso, garantizando su eficacia y continuidad en el tiempo.

¿Qué es una charla de 5 minutos y por qué es importante?

Las charlas de 5 minutos, también conocidas como **«charlas de seguridad» o «safety talks»**, son reuniones cortas realizadas al inicio

de la jornada laboral o antes de iniciar una tarea crítica. Su objetivo principal es recordar a los empleados la importancia de seguir las **normas de seguridad**, **procedimientos operacionales** y **mejores prácticas** en su entorno de trabajo.

Beneficios de la charla de 5 minutos:

- **Prevención de accidentes:** Refuerza la concienciación sobre peligros específicos y cómo evitarlos.
- **Cumplimiento normativo:** Asegura que la empresa se adhiera a regulaciones y estándares de SST y Medio Ambiente.
- **Mejora de la comunicación interna:** Fomenta la participación de los trabajadores y el intercambio de experiencias.
- **Refuerzo de la cultura de seguridad:** Mantiene la seguridad como una prioridad constante en la organización.
- **Aumento de la productividad:** Minimiza tiempos de inactividad por incidentes o errores prevenibles.

Implementación de charlas de 5 minutos en el sector empresarial

Las empresas, independientemente de su sector, pueden beneficiarse enormemente de la incorporación de charlas de 5 minutos en su rutina diaria. Sin embargo, la clave del éxito radica en su **planificación, ejecución y seguimiento**.

3 temas clave a abordar en las charlas de seguridad

Las **Charlas de seguridad** son una herramienta fundamental en la gestión de **Salud, Seguridad y Medioambiente (HSE)** dentro de las organizaciones. Se trata de reuniones breves, generalmente de **5 a 15 minutos**, cuyo objetivo es reforzar la cultura de seguridad y prevenir accidentes en el trabajo.

Implementadas correctamente, estas charlas contribuyen a la **reducción de incidentes laborales, el cumplimiento normativo y el fortalecimiento del compromiso de los trabajadores** con la seguridad.

En este artículo, exploraremos **tres temas clave** que toda empresa debe abordar en sus **Charlas de seguridad** para mejorar la prevención de riesgos laborales.

Charlas de seguridad

Las **Charlas de seguridad** permiten a las empresas **crear conciencia sobre los riesgos laborales** y fomentar la aplicación de **buenas prácticas** en el día a día.

Algunos de sus principales beneficios incluyen:

- **Reducción de accidentes y enfermedades laborales.**
- **Mejor cumplimiento de normativas de seguridad y salud en el trabajo.**
- **Mayor compromiso de los trabajadores con la prevención de riesgos.**
- **Comunicación efectiva sobre peligros y medidas de control.**

Las **Charlas de seguridad** son una herramienta fundamental en la gestión de **Salud, Seguridad y Medioambiente (HSE)** dentro de las organizaciones. Se trata de reuniones breves, generalmente de **5 a 15 minutos**, cuyo objetivo es reforzar la cultura de seguridad y prevenir accidentes en el trabajo.

Implementadas correctamente, estas charlas contribuyen a la **reducción de incidentes laborales, el cumplimiento normativo y el fortalecimiento del compromiso de los trabajadores** con la seguridad.

En este artículo, exploraremos **tres temas clave** que toda empresa debe abordar en sus **Charlas de seguridad** para mejorar la prevención de riesgos laborales.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

ESGinnova Group

GRCTools

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

Nueva Ley de Ciberseguridad y Seguridad de la Información de El Salvador

La reciente aprobación de la **Ley de Ciberseguridad y Seguridad de la Información** de El Salvador representa un paso fundamental hacia la protección de la información digital y la prevención de delitos cibernéticos. Este avance legal tiene importantes implicaciones para el sector empresarial, que enfrenta una creciente exposición a riesgos digitales en un mundo cada vez más interconectado. Con la creación de la **Agencia de Ciberseguridad del Estado (ACE)** y la implementación de un **Registro Nacional de Amenazas e Incidentes de Ciberseguridad**, se sientan las bases para una gobernanza más robusta en materia de seguridad de la información.

Aspectos clave de la nueva Ley de Ciberseguridad y Seguridad de la Información de El Salvador

La **Ley de Ciberseguridad y Seguridad de la Información de El Salvador** establece un marco normativo para la protección de datos y la prevención de ciberataques en el país.

Entre sus puntos más destacados se encuentran:

01. **Creación de la Agencia de Ciberseguridad del Estado (ACE):** Este organismo será responsable de coordinar, monitorear y gestionar la ciberseguridad en instituciones públicas y sectores críticos.

02. **Registro Nacional de Amenazas e Incidentes de Ciberseguridad:** Las organizaciones deberán notificar cualquier incidente de seguridad relevante, lo que permitirá al Estado centralizar la información sobre amenazas y mejorar las respuestas ante ataques.

03. **Obligación de cumplimiento para empresas:** Las entidades del sector público y privado deberán adoptar medidas de protección de la información, incluyendo la implementación de controles de seguridad y políticas de gestión de riesgos.

04. **Protección de infraestructuras críticas:** Se establecen directrices para asegurar sistemas esenciales en sectores clave como telecomunicaciones, energía y finanzas.

05. **Capacitación y concienciación:** La ley fomenta la formación continua en temas de ciberseguridad tanto para el sector público como privado.

06. **Sanciones:** Se contemplan sanciones para aquellas organizaciones que no cumplan con las disposiciones legales, lo que refuerza la obligatoriedad de adoptar buenas prácticas de seguridad.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Cómo se lleva a cabo la investigación de accidentes con el arbol de causas?

La gestión de riesgos es un pilar fundamental en cualquier organización que busca garantizar la **seguridad y continuidad operativa**. Cuando ocurre un accidente, es imprescindible analizar las circunstancias que lo originaron para evitar su repetición. Una de las metodologías más utilizadas en este ámbito es el **arbol de causas**, una herramienta que permite **identificar, estructurar y analizar** los factores que condujeron a un incidente.

El **arbol de causas** es un método de análisis estructurado que facilita la comprensión de los eventos previos a un accidente, estableciendo relaciones de causa-efecto de manera gráfica. Su objetivo es **determinar las causas raíz del problema** y proponer medidas preventivas eficaces. En este artículo, exploraremos cómo se lleva a cabo una **investigación de accidentes** utilizando el **arbol de causas**, sus beneficios y su aplicación en el ámbito corporativo.

Arbol de causas

El **arbol de causas** es una técnica de análisis que permite representar, en forma de diagrama, la **cadena de eventos y condiciones** que provocaron un accidente. Se basa en la premisa de que todo incidente es el resultado de una combinación de **factores múltiples**, no de un único fallo.

Características del arbol de causas

- Es una **herramienta visual y estructurada**, lo que facilita la comprensión del incidente.
- Permite **profundizar en las causas subyacentes**, más allá del error humano evidente.
- Se basa en la **lógica de preguntas sucesivas**, identificando hechos encadenados hasta llegar a la raíz del problema.
- Ayuda a **diseñar estrategias correctivas y preventivas** con mayor precisión.

Fases de la investigación de accidentes con el arbol de causas

La aplicación del **arbol de causas** en una investigación de accidentes consta de varias **etapas** bien definidas:

1. Recopilación de información

Antes de construir el arbol de causas, es fundamental recolectar todos los **datos relevantes sobre el accidente**.

¿Qué es el Decreto 143 de El Salvador?

El entorno normativo en El Salvador ha evolucionado significativamente en los últimos años para fortalecer la seguridad de la información y la protección de datos en las organizaciones. Dentro de este marco, el **Decreto 143** se posiciona como una regulación clave para el sector empresarial, estableciendo lineamientos específicos sobre la **gestión de la seguridad de la información** y el cumplimiento normativo en materia de protección de datos.

Este decreto establece requisitos fundamentales para las empresas en cuanto a la **gestión de riesgos cibernéticos**, la **implementación de medidas de seguridad**, la **gestión de incidentes** y la **protección de datos personales y corporativos**. Su objetivo principal es garantizar que las organizaciones implementen buenas prácticas en materia de ciberseguridad, alineándose con marcos internacionales como la norma **ISO/IEC 27001** y los lineamientos del **NIST (National Institute of Standards and Technology)**.

Características principales del Decreto 143 de El Salvador

El Decreto 143 establece un marco regulatorio con varios elementos fundamentales que buscan garantizar la seguridad de la información y la continuidad operativa de las organizaciones en El Salvador. Entre sus principales características se encuentran:

- **Obligatoriedad de medidas de seguridad:** Las empresas y entidades gubernamentales deben implementar controles y protocolos de seguridad informática para resguardar la integridad, confidencialidad y disponibilidad de los datos.

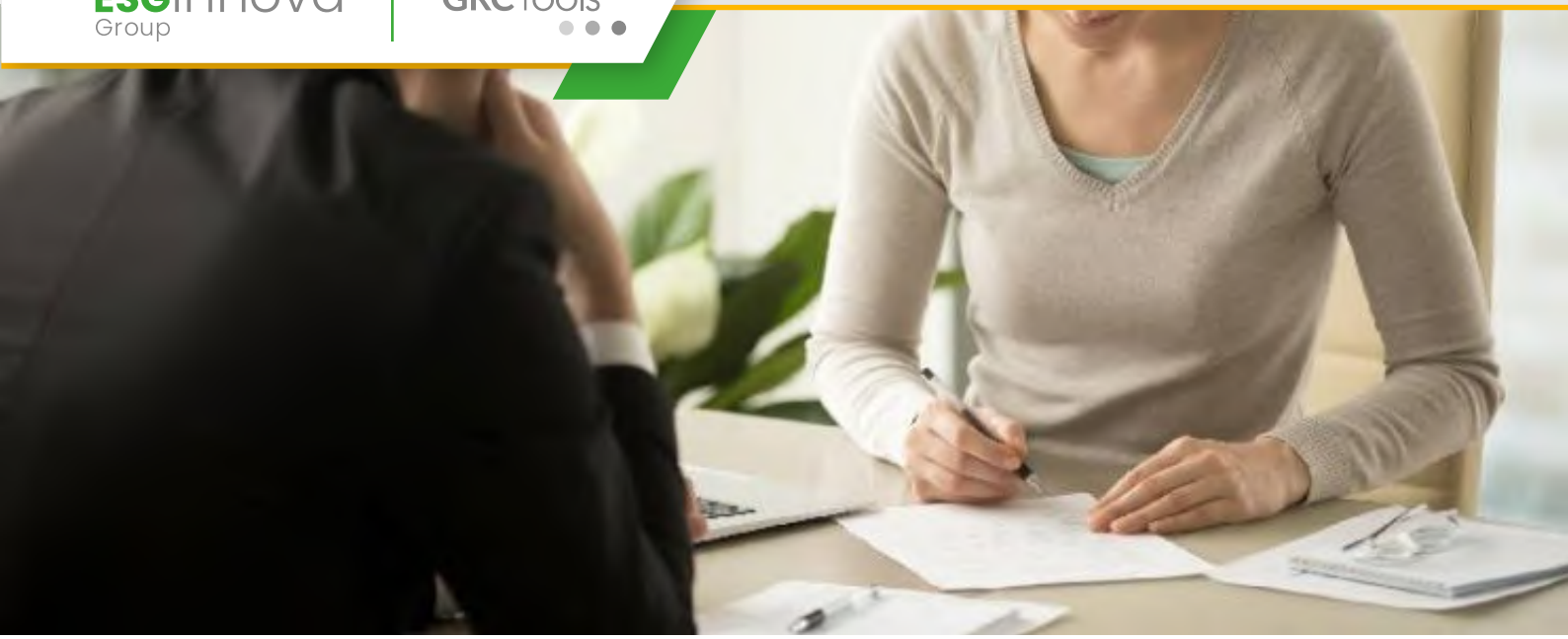
- **Gestión de riesgos de ciberseguridad:** Se exige la identificación, evaluación y mitigación de riesgos asociados a la seguridad de la información, promoviendo el uso de metodologías basadas en estándares internacionales.

- **Notificación de incidentes:** Las organizaciones están obligadas a reportar incidentes de ciberseguridad a las autoridades competentes en un plazo determinado, facilitando una respuesta coordinada ante amenazas digitales.

- **Protección de datos personales y privacidad:** El decreto incorpora disposiciones alineadas con normativas internacionales sobre privacidad, exigiendo a las empresas garantizar el manejo adecuado de los datos de clientes y usuarios.

- **Capacitación y concienciación:** Se promueve la formación continua de los empleados en materia de ciberseguridad, con el fin de reducir el riesgo de ataques derivados del factor humano.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Explicación paso a paso de la debida diligencia

En un mundo empresarial cada vez más regulado y expuesto a riesgos, la **debida diligencia** se ha convertido en un proceso indispensable para las organizaciones que buscan cumplir con normativas, proteger su reputación y minimizar riesgos legales y financieros. En este artículo, exploraremos detalladamente qué es la debida diligencia, sus pasos clave, los problemas más comunes que enfrentan las empresas en el cumplimiento normativo y cómo un **Software de Compliance**, como el Software de Debida Diligencia de GRCTools, puede optimizar este proceso.

¿Qué es la debida diligencia?

La debida diligencia es un proceso de **investigación**, **verificación** y **análisis** que permite a las organizaciones evaluar los riesgos y oportunidades antes de tomar decisiones estratégicas. Se aplica en diversas situaciones, como adquisiciones, evaluación de proveedores, cumplimiento normativo y prevención de delitos financieros.

Paso a paso de la debida diligencia

1. Definir el objetivo y alcance

Cada organización debe determinar el **propósito** de la debida diligencia: ¿es para evaluar un proveedor?, ¿para un proceso de fusiones y adquisiciones?, ¿para el cumplimiento de normativas anticorrupción? Definir estos objetivos ayudará a estructurar un proceso eficiente y enfocado.

2. Recopilación de información

Se debe obtener toda la información relevante sobre la entidad investigada, incluyendo documentos **financieros**, **legales**, **antecedentes** reputacionales y cumplimiento con **regulaciones**.

3. Evaluación de riesgos

- Se analizan aspectos clave como:
- Riesgos financieros y contables.
- Cumplimiento normativo (**anticorrupción**, blanqueo de capitales, privacidad de datos, etc.).
- Riesgos reputacionales y operativos.

4. Verificación y validación de la información

La información recopilada debe ser corroborada con **fuentes oficiales** y **auditorías** independientes para garantizar su autenticidad.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Todas las claves para cumplir con la Ley de Ciberseguridad de El Salvador

En un mundo donde la digitalización es clave para el desarrollo económico y la seguridad de la información es un pilar fundamental, los gobiernos han comenzado a establecer **normativas estrictas** para proteger los datos y los sistemas informáticos de sus países. En este contexto, la **Ley de Ciberseguridad de El Salvador**, una regulación que busca fortalecer la **protección de infraestructuras críticas, prevenir ataques cibernéticos y establecer directrices claras** para la gestión de la seguridad digital en el país.

Para las empresas y organizaciones que operan en El Salvador, el cumplimiento de esta ley no es solo una obligación legal, sino una **estrategia clave para garantizar la continuidad del negocio** y la confianza de clientes y socios. En este artículo, exploraremos las **principales disposiciones de la Ley de Ciberseguridad de El Salvador**, los **requisitos clave para su cumplimiento** y cómo las organizaciones pueden **implementar estrategias efectivas de ciberseguridad**.

Ley de Ciberseguridad de El Salvador

La **Ley de Ciberseguridad de El Salvador** es una normativa diseñada para regular el **uso, protección y gestión de los sistemas digitales** en el país. Su objetivo es **proteger la infraestructura crítica**, evitar ciberataques y establecer mecanismos de **respuesta y recuperación ante incidentes de seguridad**.

Objetivos principales de la Ley de Ciberseguridad de El Salvador

- **Proteger la información y los sistemas digitales** utilizados por el gobierno, empresas privadas y ciudadanos.
- **Fortalecer la infraestructura crítica** del país contra amenazas cibernéticas.
- **Establecer lineamientos para la gestión de riesgos de ciberseguridad** en organizaciones públicas y privadas.
- **Crear mecanismos de supervisión y control** para asegurar el cumplimiento de la normativa.
- **Fomentar la capacitación y sensibilización en ciberseguridad** a nivel nacional.

¿A quiénes aplica la Ley de Ciberseguridad de El Salvador?

La Ley de Ciberseguridad de El Salvador aplica a un amplio espectro de entidades.

¿Cuáles son los tipos de riesgos laborales más importantes? 10 ejemplos

La **gestión de riesgos laborales** es un aspecto fundamental en cualquier organización, ya que permite garantizar la seguridad y el bienestar de los trabajadores. En el marco del Gobierno, Riesgo y Cumplimiento (GRC), la identificación, evaluación y mitigación de estos riesgos son esenciales para evitar accidentes, enfermedades profesionales y pérdidas económicas.

Conocer los diferentes tipos de riesgos laborales es clave para implementar **estrategias de prevención efectivas**. Sigue leyendo para explorar los principales riesgos que pueden presentarse en el entorno laboral y su impacto en las organizaciones. Asimismo, abordaremos cómo la adopción de **soluciones tecnológicas**, como el Software de Riesgos Laborales de GRCTools, contribuye a una gestión más eficiente y a la creación de un entorno de trabajo más seguro.

Tipos de riesgos laborales y 10 ejemplos clave

Los tipos de riesgos laborales pueden clasificarse según su **naturaleza** y el **impacto** que generan en la salud de los trabajadores. A continuación, presentamos los principales tipos y ejemplos de cada uno:

1. Riesgos físicos

Factores ambientales que pueden generar daños en el organismo. **Ejemplo:** Exposición a ruido excesivo en una planta de producción, lo que puede derivar en pérdida auditiva.

2. Riesgos químicos

Exposición a sustancias tóxicas o corrosivas. **Ejemplo:** Manipulación de solventes sin equipo de protección personal en la industria farmacéutica.

3. Riesgos biológicos

Contacto con virus, bacterias u otros microorganismos peligrosos. **Ejemplo:** Personal sanitario expuesto a enfermedades infecciosas sin las medidas adecuadas.

4. Riesgos ergonómicos

Factores relacionados con posturas inadecuadas o esfuerzo físico repetitivo. **Ejemplo:** Dolor lumbar crónico en empleados de oficina debido a una mala postura frente al ordenador.

Así se elabora el mapa de riesgos de una empresa

La **gestión del riesgo** es una piedra angular en la estrategia de cualquier organización que aspire a la sostenibilidad y al crecimiento en un entorno cada vez más complejo y regulado. Un elemento clave dentro de esta gestión es el **mapa de riesgos de una empresa**, una herramienta que permite identificar, evaluar y visualizar los riesgos de una empresa para tomar decisiones informadas y mitigar posibles amenazas.

Los principales problemas del sector empresarial en la gestión del riesgo

A pesar de la creciente conciencia sobre la importancia de la gestión del riesgo, muchas empresas siguen enfrentando una serie de obstáculos que dificultan la implementación de estrategias efectivas. Entre los principales problemas destacan:

01. **Fragmentación de la información**: La falta de centralización y la dependencia de hojas de cálculo o documentos dispersos dificultan una visión integral de los riesgos.

02. **Falta de metodologías estandarizadas**: Muchas organizaciones carecen de un enfoque unificado para evaluar y tratar los riesgos, lo que conlleva inconsistencias y errores en la gestión.

03. **Desactualización de los mapas de riesgos**: Sin herramientas adecuadas, el monitoreo continuo se vuelve una tarea ardua, dejando a las empresas vulnerables a cambios en su entorno.

04. **Dificultad en la asignación de responsabilidades**: No definir claramente los responsables de la gestión de riesgos genera ineficiencias y retrasos en la **toma de decisiones**.

05. **Cumplimiento normativo deficiente**: La falta de un sistema estructurado para la gestión del riesgo dificulta el cumplimiento de regulaciones y normativas, exponiendo a la empresa a sanciones y pérdidas financieras.

Pasos para elaborar un mapa de riesgos de una empresa efectivo

Para abordar estos problemas, el mapa de riesgos de una empresa se debe estructurar adecuadamente siguiendo estos pasos:

- La elaboración de un mapa de riesgos de una empresa comienza con la **identificación de amenazas**, clasificándolas en categorías como financieras, operativas, tecnológicas, regulatorias y reputacionales. Este análisis permite reconocer vulnerabilidades que podrían afectar la empresa.

- Luego, se realiza la **evaluación del impacto y la probabilidad**, determinando la posibilidad de ocurrencia de cada riesgo y su efecto en la organización.

Siglas ASG: pilares de la sostenibilidad empresarial

En el mundo empresarial actual, la sostenibilidad se ha convertido en un factor clave para garantizar el éxito a largo plazo. Las **siglas ASG**, que representan los criterios **Ambientales, Sociales y de Gobernanza**, han adquirido una gran relevancia en la evaluación del desempeño corporativo. Inversionistas, clientes y organismos reguladores han elevado sus expectativas, exigiendo a las empresas **compromiso con el medioambiente, responsabilidad social y prácticas de gobierno corporativo transparentes**.

Pero, ¿qué significan exactamente estos criterios y cómo impactan en las organizaciones? En este artículo exploraremos los pilares de las **siglas ASG**, su **importancia** en el mundo empresarial y cómo las empresas pueden integrar estos principios para **mejorar su competitividad y reputación**.

ASG

Las **siglas ASG** hacen referencia a los factores **Ambientales, Sociales y de Gobernanza** que determinan la **sostenibilidad** y

la **responsabilidad corporativa** de una empresa. Estos criterios permiten evaluar el impacto de una organización más allá de los indicadores financieros, **analizando su compromiso** con el entorno y la sociedad.

Los tres pilares de ASG

- **Ambiental (A):** Se enfoca en el impacto de la empresa sobre el **medioambiente**, incluyendo aspectos como la reducción de emisiones de carbono, el uso eficiente de recursos y la gestión de residuos.

- **Social (S):** Evalúa el trato a **empleados, clientes y comunidades**, considerando la diversidad, inclusión, condiciones laborales y derechos humanos.

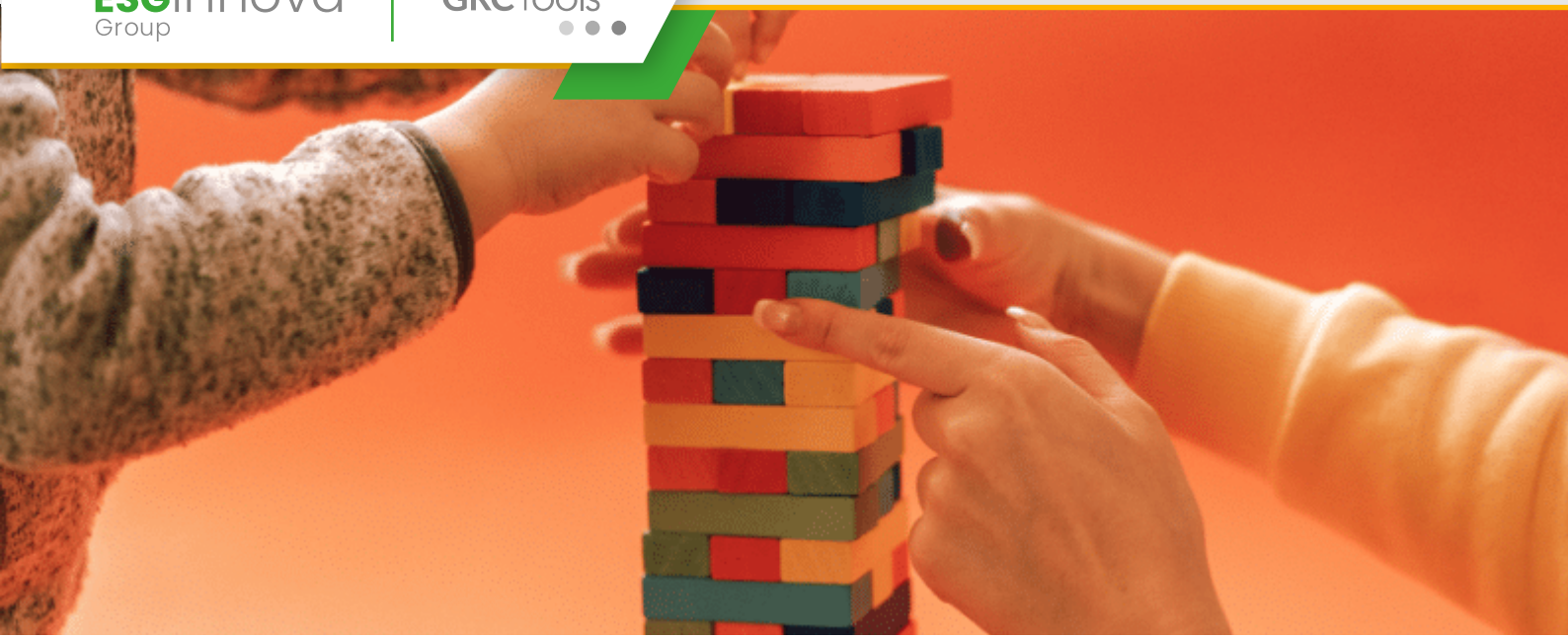
- **Gobernanza (G):** Se centra en la **transparencia, ética** y estructura de **liderazgo** de la organización, asegurando prácticas empresariales responsables y cumplimiento normativo.

Importancia de los criterios ASG en el mundo empresarial

La integración de los criterios **ASG** no es solo una tendencia, sino una **necesidad estratégica** para las empresas que buscan ser competitivas en el mercado global.

Acceso a financiamiento y atracción de inversionistas

Los inversionistas institucionales están cada vez más enfocados en empresas que cumplen con **estándares de sostenibilidad**.



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

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

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

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

Balanced Scorecard

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

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

Perspectiva financiera

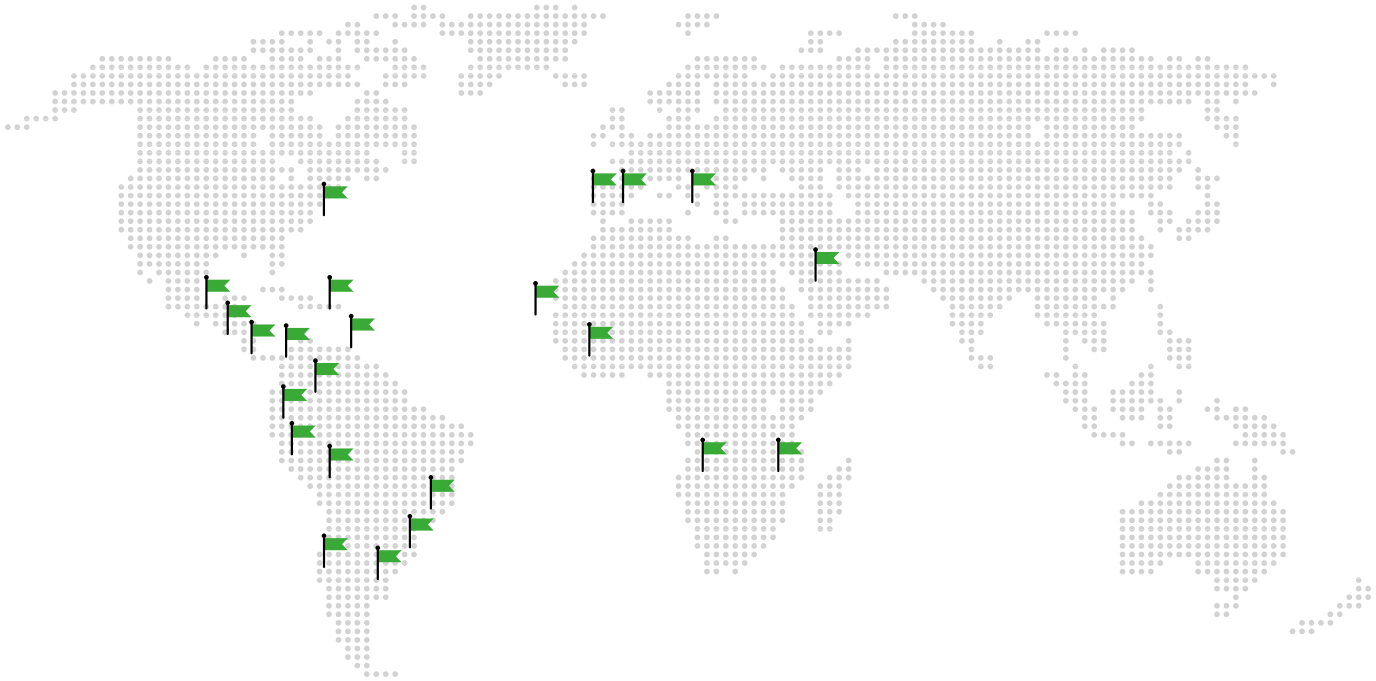
Evalúa el rendimiento económico de la empresa, considerando métricas como:

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

Perspectiva del cliente

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

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



El camino hacia la Excelencia

Desde los inicios de nuestra organización han pasado más de quince años de trabajo y mejora continua, donde el desarrollo de alianzas, la ampliación en normas y modelos, el gran crecimiento en número de clientes y tipología de proyectos, así como la expansión internacional, han marcado y marcan nuestra trayectoria.

Estamos presentes en más de quince países, en los que nuestros equipos locales prestan un servicio adaptado a la realidad y mercado de cada zona.

+2.500 organizaciones

+25 años

+30 países

+240.000 usuarios

ESGinnova
Group

Córdoba, España

C. Villnius Nº 15, P.I. Tecnocórdoba,
Parcela 6-11 Nave H, 14014
Tel: +34 957 102 000

Écija, España

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

Santiago de Chile, Chile

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

Lima, Perú

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

Bogotá, Colombia

Carrera 49,
Nº 94 - 23
Tel: +57 601 3000590 | +57 320 3657308

México DF, México

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